SecureDoc Enterprise Server

Version 9.2

クイックインストールガイド

WinMagic SecureDoc

2025 年 7 月

はじめに

SecureDoc とは、様々な OS に対応した暗号化ソフトウェアの名称です。
SecureDoc には「**スタンドアロン**」バージョンと、SecureDoc Enterprise Server（以下、「SES」という。）による「**クライアント/サーバー**」形式のバージョンがあります。
SES は、Windows や mac デバイスへ SecureDoc をインストールするために必要なインストレーションパッケージの作成や、暗号化状態の監視、セキュリティポリシーの一元管理、パスワード失念時の救済等の機能を有しており、企業での導入に適しています。

現在、多くの企業では、通常の HDD/SSD 搭載 PC の他、自己暗号化ドライブ（TCG Opal）搭載 PC、既に Microsoft BitLocker で暗号化済の PC 等、様々な環境のデバイスが存在します。情報漏洩を防ぐ為には、暗号化するだけでなく、それらの暗号化デバイスを一元管理できるソリューションが必要です。SES は、ウィンマジックの暗号化エンジンで暗号化した SecureDoc クライアントだけでなく、BitLocker で暗号化済のデバイスや自己暗号化ドライブ（TCG Opal）搭載 PC、mac、Linux のデバイスを包括的に管理できます。

本ガイドの目的

本ガイドは、SES のインストール及び基本的な設定と、Windows PC を暗号化するためのインストレーションパッケージの作成及びクライアントへのインストール方法について、説明いたします。
SES の機能、設定方法の詳細については、「SecureDoc Enterprise Server Version 9.2 リファレンス マニュアル」を、併せてご参照ください。

SecureDoc Enterprise Server Version 9.2 クイックインストールガイド

連絡先

WinMagic Inc. （カナダ本社）

200 Matheson Blvd West, Suite 201
Mississauga, Ontario, L5R 3L7
フリーダイヤル： 1-888-879-5879　電話 : (905) 502-7000　Fax : (905) 502-7001
テクニカルサポート : support@winmagic.com

ウィンマジック・ジャパン株式会社

〒105-0022
東京都港区海岸 1-2-3　汐留芝離宮ビルディング 21 階
電話 : 03-5403-6950　Fax : 03-5403-6953
営業 : sales.jp@winmagic.com　テクニカルサポート : support.jp@winmagic.com
URL : https://www.winmagic.co.jp/　https://winmagic.com/ja/home-jp/　(グローバル)

更新履歴

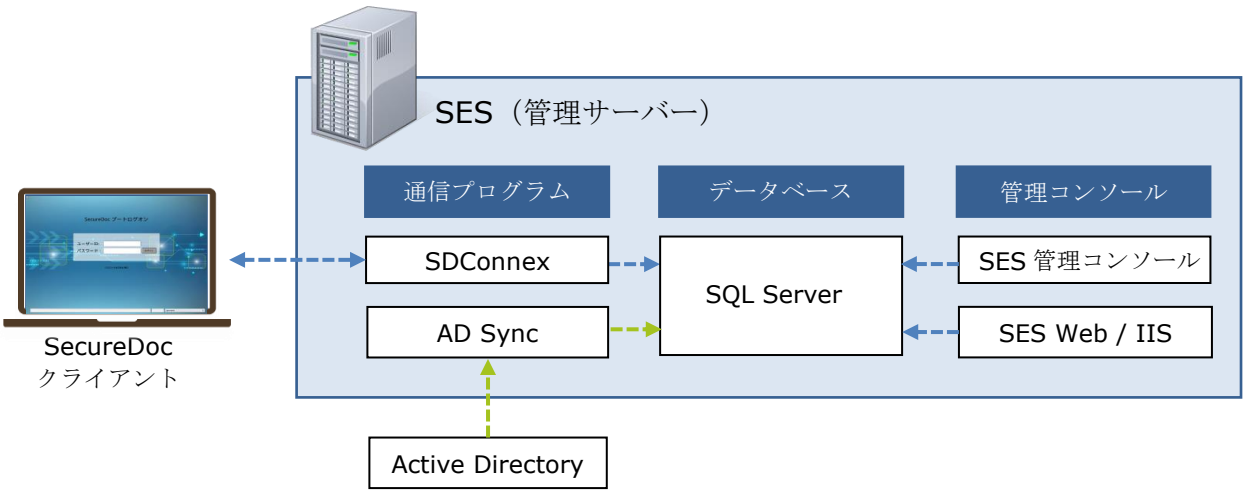
日　付	バージョン	更新内容
2025 年 7 月	初版	

※　設定画面の説明で、一部、旧バージョンの GUI（画像）が使われている場合があります。

目 次

1. SecureDoc Enterprise Server（SES）の構成

SES は、通信プログラム、データベース、管理コンソールの 3 つのコンポーネントで構成されています。それぞれを別のサーバーにインストールすることも、同一のサーバーにインストールすることもできます。



1.1. 通信プログラム

SDConnex

SDConnex は、SecureDoc クライアントと SES が通信するためのプログラムです。
SecureDoc クライアントの導入時に、クライアントデバイスで SecureDoc のインストーラーを実行すると、ディスクの暗号化に必要な「一意」の鍵の生成やユーザーID の作成はクライアント側で行われます。それらの情報は、デバイスのインベントリ情報とともに、SDConnex を経由して、SQL のデータベース（SES DB）に登録されます。
SecureDoc クライアントは、OS 起動時に SDConnex と通信しプリブート認証のログインログを送り、自分宛のコマンドがあるかを確認します。OS 起動後の定期的な通信では SES から自分宛のコマンドがあるかを確認します。管理者が SES 管理コンソールを使っておこなうコマンド（設定変更、ID の追加削除等）を、SecureDoc クライアントは OS 起動時、あるいは OS 起動後の定期的な通信で受け取ります。

SecureDoc クライアントが主に社外で利用され、社内 LAN に設置されている SDConnex と通信できない場合、SES からのコマンドを受け取ることはできませんが、クライアントデバイスの利用に支障は生じません。例えば、ユーザーのパスワード失念時、SecureDoc クライアントのパスワードリカバリーは、SDConnex と通信できない環境においても可能です

※ SDConnex は、通常、同時に 100 セッションを処理できます。
SecureDoc クライアントが SDConnex と接続できなかった場合、クライアントは接続のリトライを試みます。

※ SDConnex は、必要に応じて複数設置することができます。
例えば、社内用と社外用にそれぞれの SDConnex を設置する場合や、障害時の対策として、システム内に SDConnex を複数設置することもできます。SecureDoc クライアントが SDConnex と通信する時間はほんの一瞬なので、通常、ネットワークに負荷をかけることはありませんが、負荷分散や障害時の対策として、SDConnex を

複数設置し、SecuerDoc クライアントが最初に通信を試みる SDConnex に優先順位をつけて指定することもできます（ランダム指定も可）。
クライアントデバイスが 3,000 台以上の場合は、SDConnex を 2 台以上設置されることを推奨します。
デバイスのローカルでおこなう通常の「プリブート認証」ではなく、「プリブートネットワーク認証」を利用する場合も、SDConnex を 2 台以上設置されることを推奨します。プリブートネットワーク認証については、「SecureDoc Enterprise Server Version 9.2 リファレンス マニュアル」をご参照ください。

※ SDConnex は、Windows のサービスとして起動するため、ISV 製のサービス監視プログラム（死活ツール）等を使って監視・制御することも可能です。

AD Sync

AD Sync を利用すると、Active Directory のユーザーアカウントを SES のデータベースにインポートできます。インポートするユーザーアカウントは OU 単位で指定でき、AD Sync は Active Directory と定期的に同期します。

※ SecureDoc クライアントのインストーラーは、インストールプロセス中に、そのデバイスにサインインしている ID を参照して、同名の SecureDoc ユーザーID を自動で作成します。その ID は SDConnex を経由して SES DB に登録されますが、同名の ID が既に SES DB に存在した場合、ID の情報をマージすることができます。本機能により、Active Directory のユーザーアカウントに含まれる情報が SecueDoc のユーザーID にマージされます。

※ オプションの MagicEndpoint を使用する場合、SES に登録されている個々のユーザーID にメールアドレスの情報が必要です。Active Directory のユーザーアカウントにメールアドレスの情報が含まれている場合、AD Sync でメールアドレスをインポートできるので、管理者は個々のユーザーID にメールアドレスを追記する手間が省けます。

※ ドメインに参加していないワークグループ環境の場合、AD Sync は必要ありません

注 AD Sync をインストールしているサーバーはドメインメンバーとなる必要があります。

1.2. データベース

SES のデータベースは、マイクロソフトの SQL Server を使用します。
管理者の操作は、全て SES 管理コンソールでおこなうため、SQL データベースを直接操作する必要はありません。
データベースには、SecureDoc クライアントのユーザー、デバイス、暗号鍵の他、クライアントのインストール・設定に使用するプロファイルやインストレーションパッケージ、プリブートログ等、全ての情報が保存さます。

※ 無償で提供されているエディションの SQL Server Express も使用可能です。
SES はハイスペックなサーバー環境を必要としませんが、SQL Server Express の場合、データベースの容量が 10GB に制限されている、ジョブスケジューラ機能を利用できない点など、制約事項があります。

注 データベースを消失すると、すべてのクライアントの情報を失うため、必ず DB のバックアップを取るようにしてください。SQL のインストール時に、管理ツールの SQL Management Studio（SSMS）もインストールしておくことを推奨します。SSMS あるいは SQL Management Studio Express で、SES の DB を簡単にバックアップできます。

1.3. 管理コンソール

SES 管理コンソール

SES 管理コンソールは、OS 上で実行する Windows ネイティブの管理コンソールです。
SES コンソールにはキーファイルを使ってログインし、SQL に接続します。SecureDoc のポリシーを設定するプロファイルや、展開するためのインストレーションパッケージの作成、クライアントのリモート制御、パスワードリカバリー等の操作が可能です。管理者は SES 管理コンソールを常時起動しておく必要はありませんが、SecureDoc クライアントの利用者がパスワードを失念した際のパスワードリカバリーは管理コンソールでおこなうため、すぐに利用できる環境に置いておく必要があります。複数の管理者で管理する場合等、管理コンソールのみを複数のサーバーにインストールすることもできます。

SES Web

Web ベースの管理コンソールです。Cloud 上の VM を管理するためには必ず必要です。
オフィス内では、Windows ネイティブの SES 管理コンソールを使い、リモートでは SES Web を使うといった運用も可能です。SecureDoc クライアントの利用者がパスワードを失念した際のパスワードリカバリーも SES Web で対応できます。

1.4. その他

Analytics Engine

v8.5 から追記された機能で、SES Web に表示される分析値に使用します。
SES Web を使う場合、インストールするようにしてください。

2. SecureDoc の用語

キーファイル

通常、ディスク（HDD/SSD）の暗号化に使用する鍵は、デバイス毎に異なる「一意」のものを使います。複数のデバイスのディスクを同じ鍵で暗号化してしまうと、ユーザーの不注意等で認証情報が洩れた場合、複数のデバイスに不正アクセスされる可能性があるためです。SecureDoc は、クライアントへのインストールプロセス中に、デバイス毎に一意の鍵を自動で生成します。

AES で暗号化されたディスクの暗号化には、容易に復号化されないように、多段で暗号（復号）化する仕組みがあります。DEK（Data Encryption Key）で暗号化されたディスクを復号化するためには、必ず、KEK（Key Encryption Key）が必要です。SecureDoc では、KEK をキーファイルの中に格納し、キーファイルは、Windows からは不可視の（ディスクの）システム領域に保存します。キーファイルには、KEK のほか、キーファイルにアクセスするためのユーザー情報（ID、パスワード、権限）等が含まれています。

キーファイル

プリブート認証とキーファイル


プリブート認証

電源を入れると、OS 起動前に「プリブート認証」プログラムが実行されます。ユーザーが入力する ID/パスワードにより、キーファイル内の KEK は一時的に復号化され、内部の DEK を利用できるようになります。DEK によってディスクは復号化され、Windows を起動できます。
それぞれのデバイスは一意の DEK で暗号化されているため、デバイス毎のキーファイルに含まれる KEK は異なります。ID/パスワード入力による、この操作を「ブートログオン」とも呼びます。

キーファイルには、我々が日常で使用するキーフォルダと同じように、複数の錠（KEK）を含めることができます。ローカルディスクの暗号化だけを目的として導入する場合、キーファイルに含まれる錠は 1 つだけです。ローカルディスク以外に、サーバーの共有フォルダにあるファイルや USB メモリ等を暗号化する社内ポリシーの場合、それぞれの復号化に必要な錠をキーファイルに格納することができます。
複数の錠が格納されているキーファイルのユーザーは、「プリブート認証」での 1 度の ID/パスワード入力だけで、複数の錠を利用できます。それにより、Windows 起動後、暗号化済の USB メモリや共有フォルダにアクセスしても、暗号化を認識・意識する必要がありません。キーファイルという仕組みは、SecureDoc が持つ大きな特長の 1 つです。

複数の錠を含めた
キーファイル

注　通常、コンピューターのディスクやデータ、メディアの暗号化において、「錠」という表現が使われることはありません。本章では、SecureDoc の暗号化の仕組みをわかりやすくするために、「錠」という単語を使っていますが、他の章や他のドキュメント類では、「鍵」という表記で統一しています。

共有鍵とキーファイル

複数のユーザーが共有するフォルダや USB メモリ等のデバイスを暗号化する場合は、ローカルディスクの鍵は一意のものなので、それとは別に、SecureDoc ユーザー間で共有する錠が必要となります。SES 管理コンソールで鍵を生成し、それをクライアント利用者で共有します。本ガイドでは、それを「共有鍵」と称しています。

デバイスには、複数のキーファイルを登録することもできます。例えば、A さんのキーファイルで設定済のデバイスに、SES 管理コンソールを使って、B さんのキーファイルを追加することができます。複数のキーファイルを登録する例として、管理者のキーファイルがあります。通常、ユーザーが利用するキーファイルの権限には、ローカルディスクの復号化等の管理者に該当するような権限は含めません。管理者のキーファイルは、必要に応じて、インストール時に登録することもでき、SES 管理コンソールを使って、後からデバイスへ配信し登録することも可能です。

注　SecureDoc に限らず、暗号化ソフトウェアで使用する「錠」は、デバイスのメモリ上にロードされるため、Windows のスリープモードは推奨されません。

プロファイル

プロファイルは、SecureDoc の動作を定義する設定情報です。暗号化の対象やサーバーとの通信に必要なネットワーク設定、USB メモリを挿入した時に自動的に暗号化を開始するようなポリシー等を定義します。

1 台のデバイスに複数のキーファイル（ユーザー情報）を保存できるのに対して、プロファイルは 1 台にひとつだけ適用できます。キーファイルや鍵はインストールの過程で自動的に生成されますが、プロファイルにはインストールに必要な情報も含まれるため、インストレーションパッケージを作成する前に SES で作成する必要があります。

セキュリティポリシーの変更が必要になった場合でも、SES 管理者は、SDConnex を介して、異なるポリシーのプロファイルに変更することができます。

エマージェンシーディスク

エマージェンシーディスクは、プリブート認証プログラムに障害が発生した場合に備えて、ブートログオンに必要な情報をバックアップする機能です。プリブート認証プログラムが壊れると、OS を起動できなくなり、データを失う可能性があります。インストールと暗号化が正常におこなわれたデバイスのエマージェンシーディスクは、SDConnex 経由で SES の DB に自動で保管されています。

3. SecureDoc プリブート認証プログラムの特長

プリブート認証（PBA: Pre Boot Authentication）とは、OS 起動前におこなわれるユーザー認証のことです。プリブート認証でログインすることを ”ブートログオン” とも言います。SecureDoc をインストールすると、ディスクの UEFI ブートオーダー、あるいは MBR（マスターブートレコード）を変更し、電源を入れると、プリブート認証プログラムが起動するようになります。OS が起動する前に、ユーザーに認証を要求することで、不正な第三者が OS を起動するのを防ぎます。

※ SecureDoc のプリブート認証プログラムは、Windows プログラムの一部ではないため、OS のネイティブ認証およびアクセスコントロールのメカニズムに依存しない仕様が求められる場合でも要件を満たすことができます。

特長：

- ID / パスワードによる認証（パスワードルールの適用）の他、PIN による認証も可能
- 二要素認証（USB トークン等）および、TPM によるキーファイル保護
- ユーザーロック機能（認証失敗を繰り返した場合、SDConnex と設定された期間内に通信がなかった場合）
- シングルサインオン（Windows サインイン、MagicEndpoint へのログイン）
- SES コンソールを使ったチャレンジレスポンスによるパスワードリカバリー
- 認証にキーファイルを使うため、一度の認証で複数の鍵を使用可能（何度もパスワードを要求されません）
- 自動ログイン機能（Auto Boot）：認証をスキップし、PC を起動させる機能の実装（常に、一時的に）
- プリブートネットワーク認証（PBNA: Pre Boot Network Authentication ）
- BitLocker をサポート：BitLocker 暗号化済デバイスに SecureDoc プリブート認証プログラムを追加
- TCG Opal 1.0/2.0 自己暗号化ドライブ（HDD/SSD）をサポート

  自己暗号化ドライブにはいくつかの仕様がありますが、Opal は、TCG（Trusted Computing Group）により策定された自己暗号化ドライブの仕様で、多くのドライブベンダーが Opal をサポートしています。
  Opal の仕様を満たしている自己暗号化ドライブでも、Opal モードとして実行させるためには、Opal 対応アプリケーションによるプリブート認証プログラムが必須です。
  自己暗号化ドライブの工場出荷時の状態では、通常、「Block SID」、あるいは「HDD パスワード」を設定することができますが、プリブート認証プログラムはありません。
  Opal 対応アプリケーションの SecureDoc を使って、Opal モードをアクティベーション（ソフトウェアの機能で暗号化はおこないません）すると、ソフトウェアで暗号化するドライブと同様に、プリブート認証プログラムによるパスワードルール等のポリシーを適用できます。

  ウィンマジックは、ストレージメーカーと協力して、互換性テストを実施しています。

  https://winmagic.com/en/data-security-support/drive-compatibility/

  注 「Block SID」、「HDD パスワード」の設定は、無効にしてください。
  それらが設定されていると、Opal モードにアクティベーションできません。

  注 一部の PC で、「Block SID」を無効にできないことが報告されています。
  「Block SID」の無効化設定については、PC メーカーにご確認ください。
  無効にできない場合、Opal モードにアクティベーションできない為、ソフトウェアで暗号化する必要があります。

4. 動作要件

最新の動作要件は、Web サイトで、ご確認ください。

動作要件： https://winmagic.com/ja/data-security-support-jp/system-requirements/

ウィンマジックでは、デバイスの検証結果を公開しています。

デバイスの互換性： https://winmagic.com/en/data-security-support/device-compatibility/

5. （重要）旧バージョンから、アップグレードされるお客様へ

アップグレードされる前に、必ず、下記の注意事項をご確認ください。

注 SES Web の機能改善の為、「URL Rewrite」プラグインを IIS にインストールする必要があります。
旧バージョンで、SES Web をお使いのお客様は、v9.0 SR1 以降へアップグレードする前に必ず「URL Rewrite」をインストールしてください。

ダウンロードリンク： https://www.iis.net/downloads/microsoft/url-rewrite

インストール後、インターネット インフォメーション サービス（IIS）マネージャーを起動し、「URL 書き換え」が有効になっていることを確認してください。
「URL Rewrite」がインストールされていない状態で、SES をインストールすると、SES のインストーラーがそれをダウンロードし自動でインストールをおこないますので、インターネットに接続されている必要があります。

6. SES インストールの事前準備

SES をインストールする前に、Microsoft SQL Server をインストールしてください。SES Web を利用する場合は、IIS のインストール・設定も必要です。

注　SES に必要な Windows のコンポーネント（Microsoft Visual C 2017 Redistributable x86、Microsoft .Net Framework 等）が不足している場合、SES のインストーラーは、SES をインストールする前に、それらを Web サイトからダウンロードしてインストールします。それにはインターネット接続が必要です。

注　MagicEndpoint IdP（Identity Provider）を使用する場合、SES Web が必要です。
管理者登録の設定に SES Web を使用します。

6.1. SES で使用するアカウント

SES では単一のサービスアカウントを使用することをお勧めします。
SES のサービスを開始するために使用されるため、SES サーバー上のローカル管理者としての権限を付与する必要があります。このアカウントには、固定された強固なパスワードを持つべきで、パスワードを設定するときは、次の特殊文字を避けてください。

o ‘” ¥%_

これは、SQL インジェクション攻撃に使用される可能性があるためです。
また、SES のデータベースにアクセスするには、SQL サーバーへのアクセス権が付与されている必要があります。
SQL サーバーに対する「sysadmin」権限を付与してください。
アカウントは、Web コンソールのアプリケーションプールを起動するためにも使用します。

6.2. Microsoft SQL Server のインストール

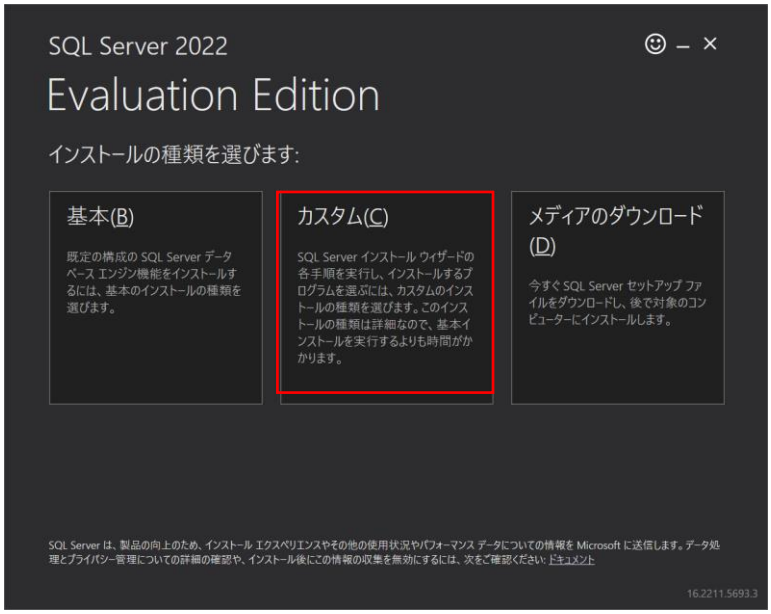
SQL Server Management Studio (SSMS)を、Microsoft SQL Server もしくは Microsoft SQL Server Express Edition と共にインストールしてください。SSMS は、SQL の設定変更時に必要で、SES DB のバックアップをとることもできます。

（ご参考）SQL Server 2022 Express の設定

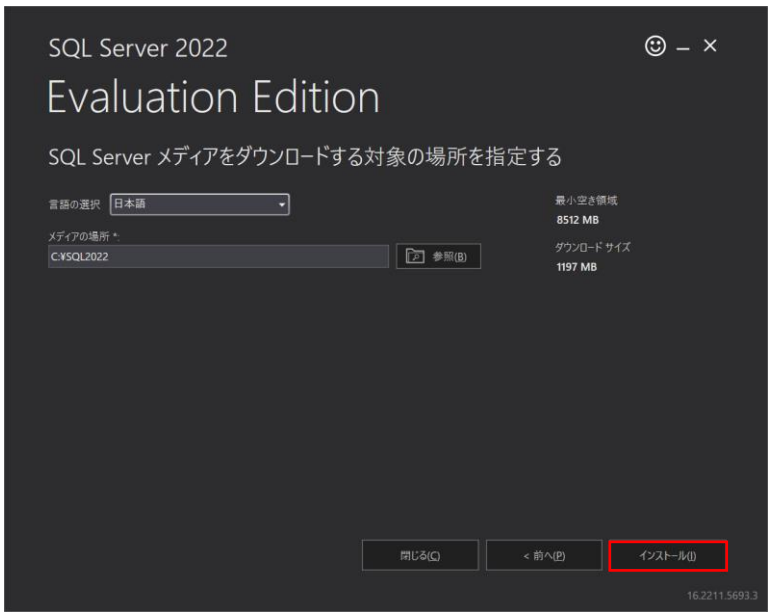
SES のデータベース作成に必要な SQL のインストール及び設定について簡単に説明します。より詳しい Microsoft SQL Server のインストールや設定方法等については、マイクロソフト社の Web サイトでご確認ください。

SQL Server 2022 Express のダウンロードリンク（ご参考）：
https://www.microsoft.com/ja-jp/sql-server/sql-server-downloads。

① マイクロソフト社のサイトからダウンロードした SQL Server 2022 Express（例：SQL2022-SSEI-Expr.exe）を実行します。インストールの種類で、[カスタム] を選択します。



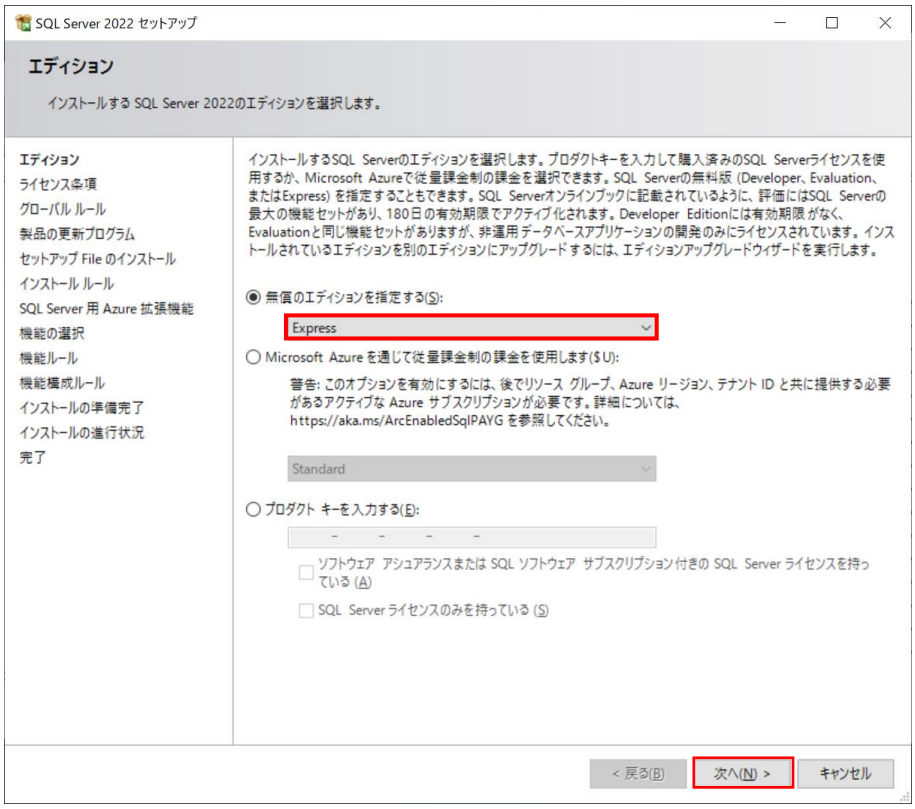
② <インストール>をクリックします。



③ 「SQL Server インストールセンター」で、[インストール] をクリックします。

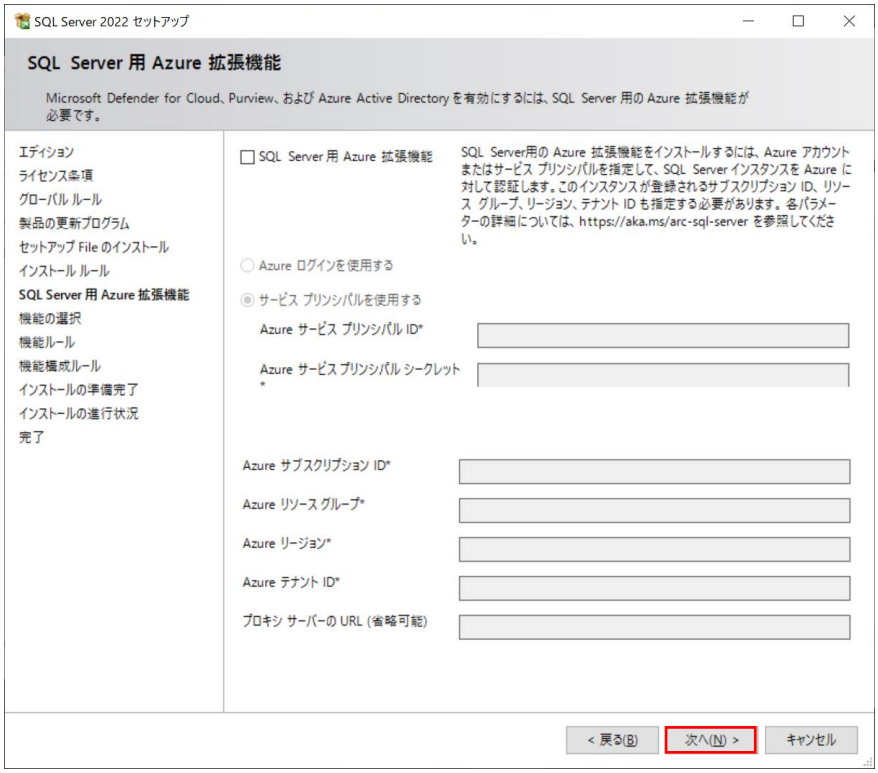
④ [SQL Server の新規スタンドアロン インストールを実行するか、既存のインストールに機能を追加] をクリックします。

⑤　エディションの選択で、プルダウンメニューから［Express］を選択し、<次へ>をクリックします。



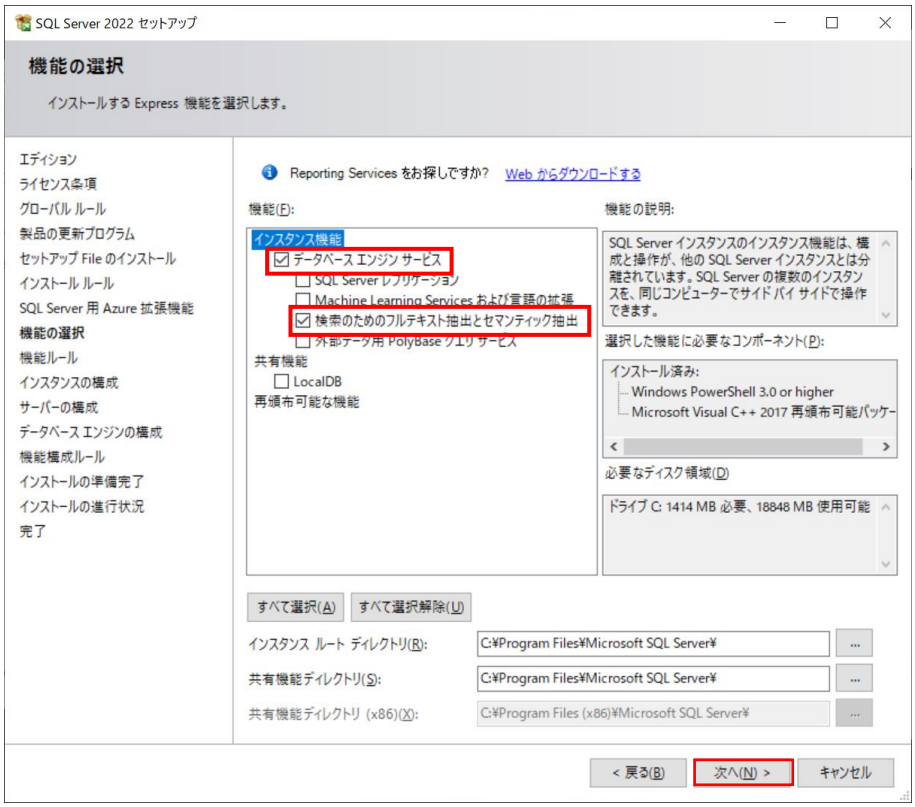
⑥　[ライセンス条項と次に同意する]を確認し、<次へ>をクリックします。

⑦ Azure 拡張機能の設定画面が表示されます。SES では使用しません。不要であればチェックを外します。
<次へ>をクリックします。

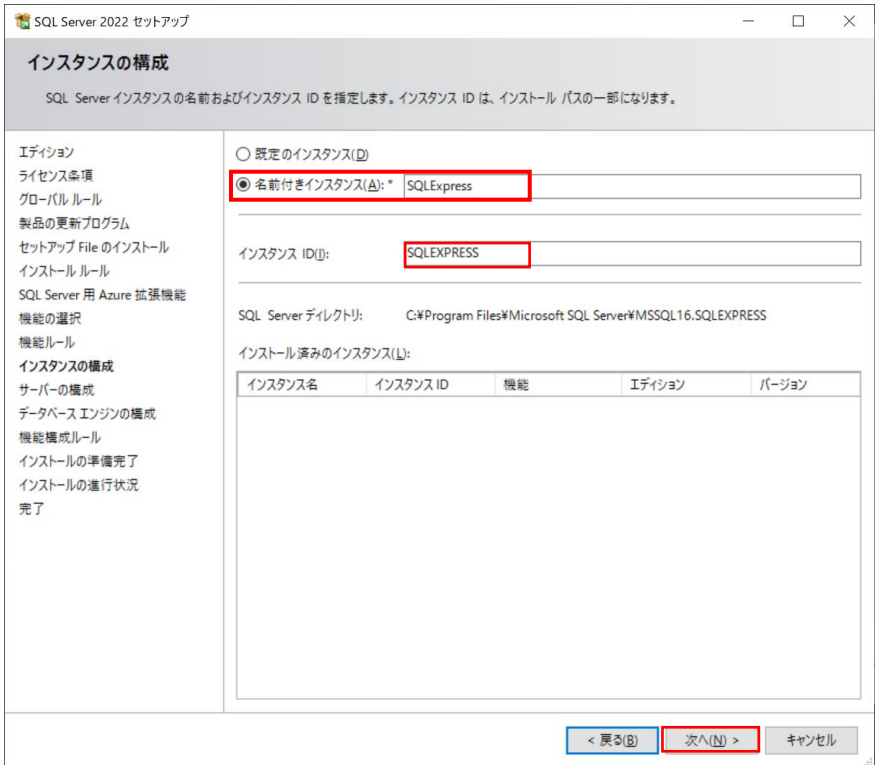


⑧ 「機能の選択」で、必ず下記の 2 つは選択してください。

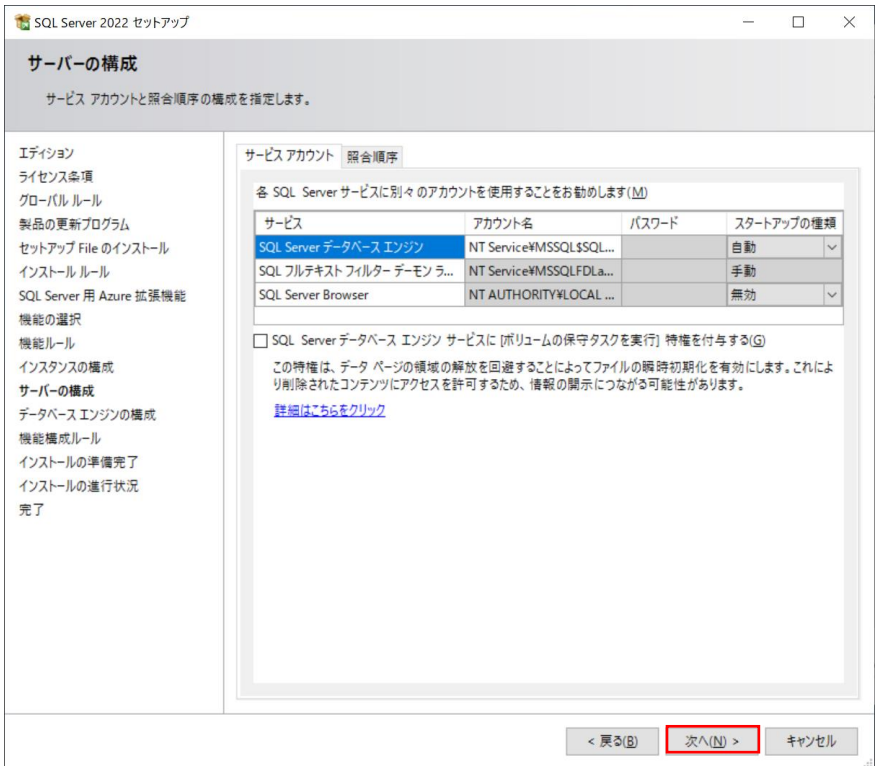
☑ データベースエンジンサービス
☑ 検索のためのフルテキスト抽出とセマンテック抽出



⑨ 「インスタンスの構成」で、[名前付きインスタンス：SQLExpress] を選択します。
「名前付きインスタンス」と「インスタンス ID」は、変更せず、SQLEXPRESS のままにします。



⑩ 「サーバーの構成」では、変更の必要がなければ、そのまま<次へ>をクリックします。

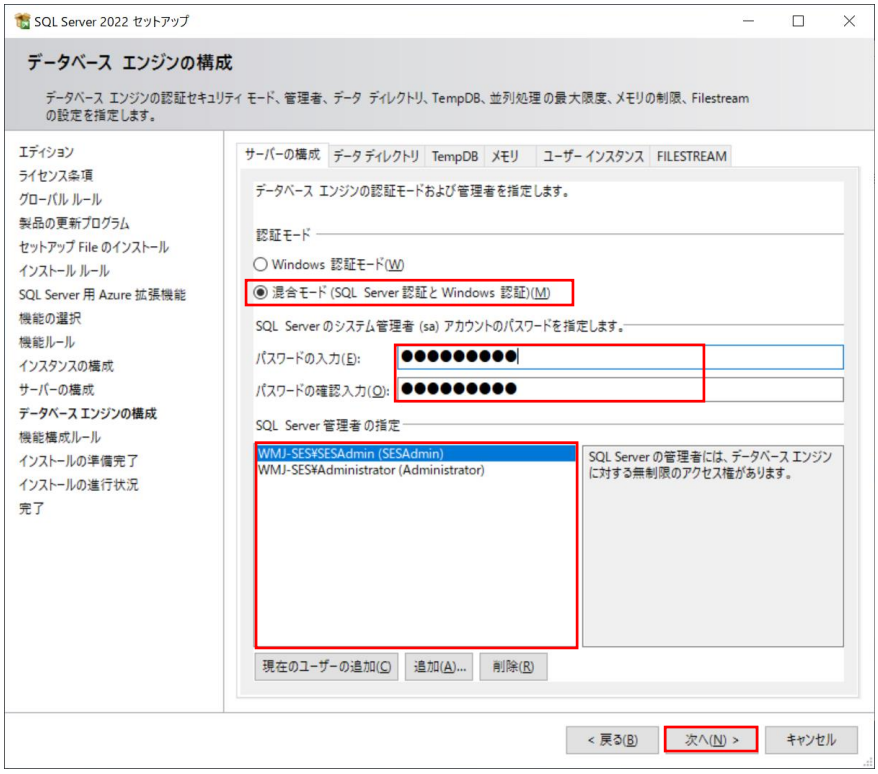


⑪ 「認証モード」で、[混合モード（SQL Server 認証と Windows 認証）] を選択します。

「sa」アカウントに強固なパスワードを設定します。

「SQL Server 管理者の指定」で、Windows 認証で使用する管理者を追加します。

「6.1.SES で使用するアカウント」で作成した管理者を追加してください。



※ 通常は Windows 認証を使用しますが、SQL へのログインに不具合が発生した場合など、SQL Server 認証（sa）でログインできる環境にしておくことで、問題回避に役立つ場合があります。

※ 認証モードの選択については、マイクロソフト社の Web サイトをご参照ください。

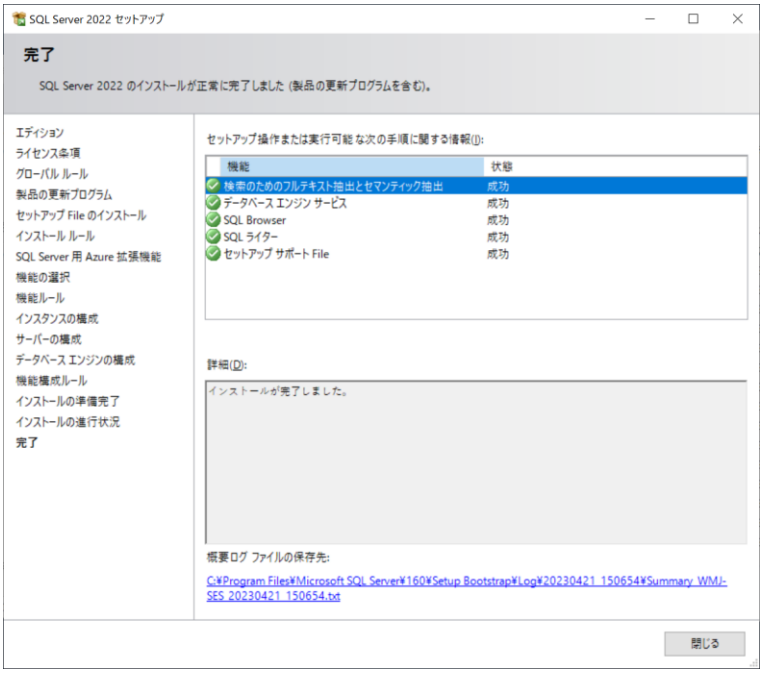
https://docs.microsoft.com/ja-jp/sql/relational-databases/security/choose-an-authentication-mode?view=sql-server-ver16

メモ：

sa アカウントのパスワード	

⑫　ここまでで、インストールの準備が完了したので、<インストール>をクリックします。

⑬　正常にインストールが完了すると、下図のように表示されます。



⑭　次に、SQL Server Management Studio (SSMS)をインストールしてください。

SSMS のダウンロードリンク（ご参考）：

https://learn.microsoft.com/ja-jp/ssms/install/install

6.3. IIS のインストールと設定

SES Web を使用する場合、SES のインストール前に、IIS のインストール・設定が必要です。

注　IIS のインストール後、「URL Rewrite」プラグインをインストールする必要があります。

① [スタート] > [サーバーマネージャー] を実行します。

② 「ダッシュボード」から「このローカルサーバーの構成」で [役割と機能の追加] をクリックします。「役割と機能の追加ウィザード」を起動します。画面の指示に従って、先に進みます。

③ 「サーバーの役割」で、[☑ Web サーバー（IIS）] を選択し、<機能の追加>をクリック後、<次へ>を数回クリックすると、「Web サーバーの役割（IIS）」の設定画面が表示されます。

④ 次の役割を追加してください。

☑ Web サーバー
- ☑ アプリケーション開発
- ☐ .Net 拡張機能 3.5
- ☑ .Net 拡張機能 4.8
- ☑ Application Initialization
- ☑ ASP
- ☐ ASP.Net 3.5
- ☑ ASP.Net 4.8
- ☐ CGI
- ☑ ISAPI フィルター
- ☑ ISAPI 拡張
- ☑ WebSocket プロトコル
- ☑ サーバー側インクルード

⑤ 「URL Rewrite」プラグインを IIS にインストールしてください。

URL Rewrite ダウンロードリンク（ご参考）： https://www.iis.net/downloads/microsoft/url-rewrite

⑥ インストール後、インターネット インフォメーション サービス（IIS）マネージャーを起動し、「URL 書き換え」が有効になっていることを確認してください。

6.4. Microsoft .NET Framework 4.7.2 以降 のインストール

Microsoft .NET Framework 4.7.2 以降が必要です。
最新の.NET は、マイクロソフト社からダウンロードしてインストールしてください。

7. SES のインストール

インストール前に Microsoft SQL Server 及び必要なソフトウェアがインストール済であることを確認してください。

注　インストール途中で、下記のアラートメッセージが表示された場合、SQL に「検索のためのフルテキスト抽出とセマンテック抽出」がインストールされていません。

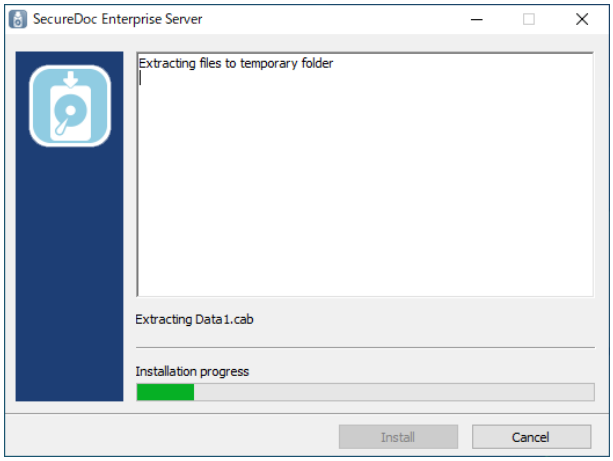
FullText Search is currently not enabled for this SQL server (required by Webserch).

We strongly recommend to enable FullText Search before creating/upgrading database.

インストールを中止して SES をアンインストールし、「検索のためのフルテキスト抽出とセマンテック抽出」を有効にしてから、SES を再インストールしてください。

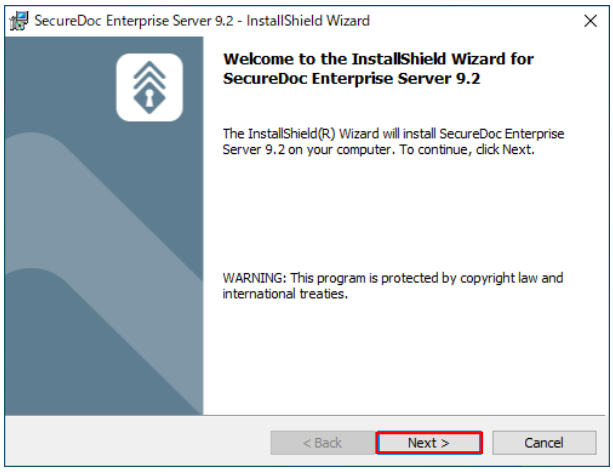
手順：

①　「SES_9.2*****.exe」を Windows の管理者権限で実行してください。プログラムの解凍が始まります。ファイル名は、バージョン（サービスリリース等）により異なります。



※　SES のインストーラーが Windows Defender SmartScreen によってブロックされた場合、[詳細情報] をクリック後に、表示された画面で<実行>をクリックするとインストールを開始することができます。

②　インストールウィザードが起動します。開始するには<Next>をクリックします。

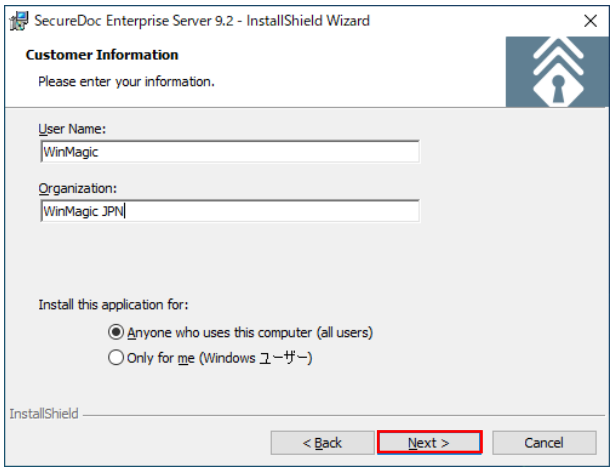


③ ライセンス契約の画面が表示されます。

使用許諾契約の内容に同意して、インストールを進めるには、[I accept the terms in the license agreement]を選択し、<Next>をクリックします。

④ SES を利用するユーザー情報の入力画面が表示されます。

ここで Windows にログインしているアカウントに限定する場合は、[Only for me(***)]を選択します。



⑤ 必要な情報を入力後、<Next>をクリックします。

⑥ インストールする SES のコンポーネントを選択します。

1 台のサーバーで SES を構築する場合、必ず、SecureDoc Enterprise Server と SDConnex/ADSync をインストールしてください。

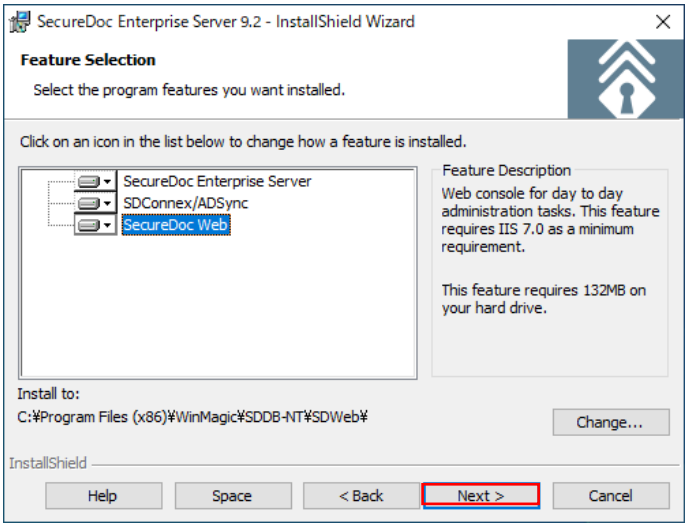
各コンポーネントは、それぞれ別のサーバーにインストールすることもできます。

 のドロップダウンから、[**X**]を選択すると、そのコンポーネントはインストールされません。

例えば、コンソールの SecureDoc Enterprise Server のみをインストールして、別のサーバーに SDConnex をインストールする場合や、SDConnex を複数設置する場合等は、必要なコンポーネントのみを選択します。

SecureDoc Web（SES Web）を利用する場合、事前に IIS が設定されている必要があります。

<Next>をクリックして、次へ進みます。

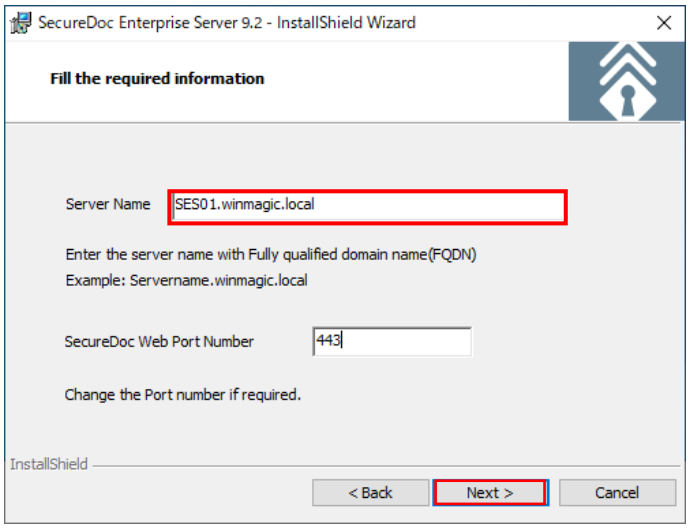


※ SecureDoc Web を選択した場合、次の画面が表示されます。

インストーラーは、自動でコンピューター名を取得し、「Server Name」にインプットします。

SecureDoc Web Port Number は、デフォルトで 443 が入力されています。

SSL の通信では、HTTPS の 443 番ポートを利用します。



注 SecureDoc Web を正しく設定する為に、必ず、正確な FQDN 名に変更してください。

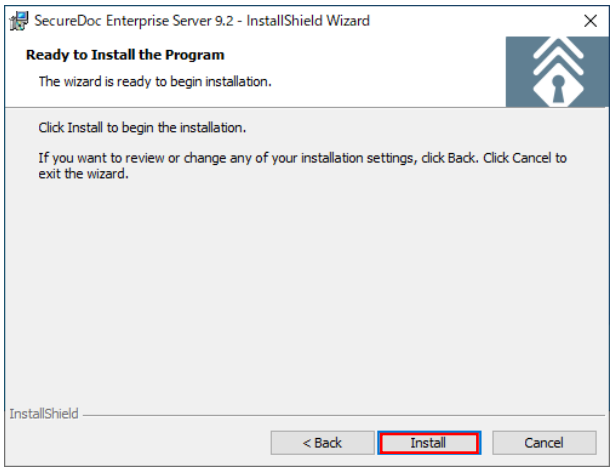
例）ses01.winmagic.local

メモ：

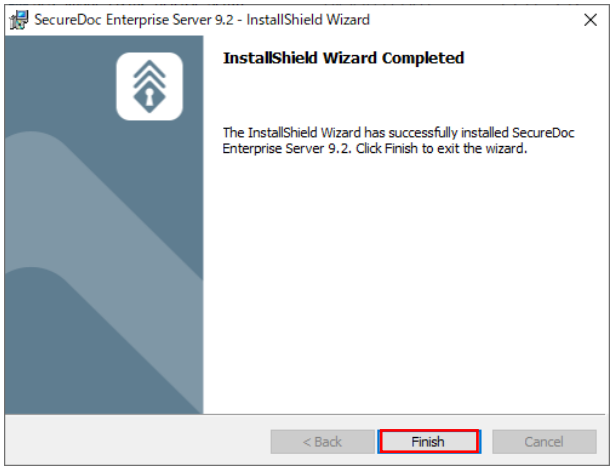
Server Name	
SecureDoc Web Port Number	

⑦ <Next>をクリックします。

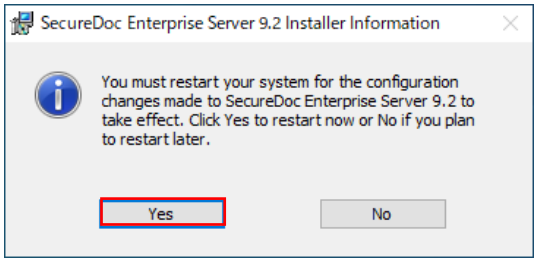
⑧ <Install>をクリックして、インストールを開始します。



⑨ 次の画面が表示されれば、正しくインストールが完了しました。<Finish>をクリックしてください。



⑩ 起動を要求されます。<Yes>をクリックし、再起動してください。



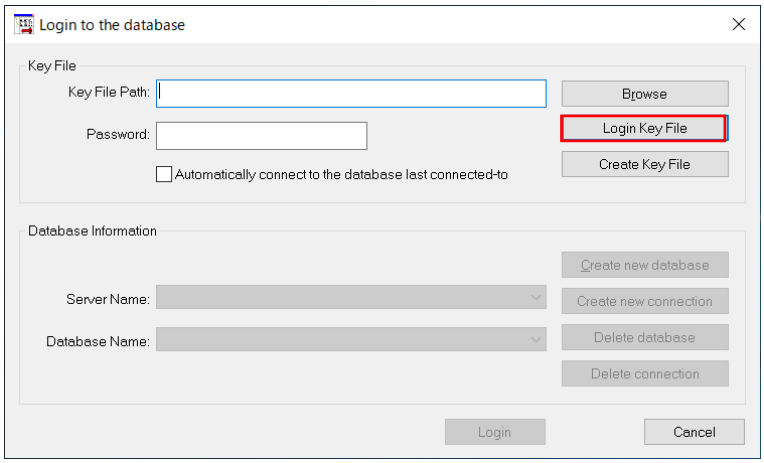
8. SES の初期設定

8.1. 管理者用キーファイルとデータベースの作成

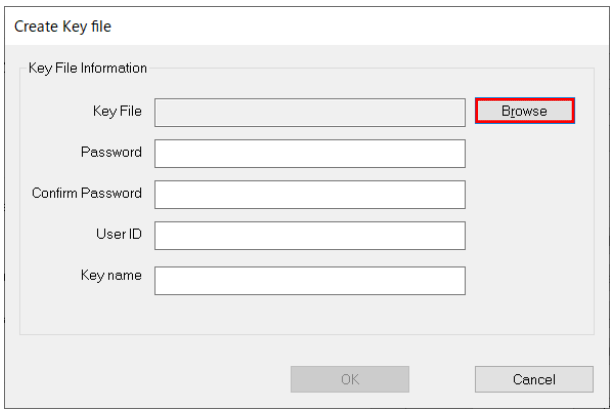
最初に SES にログインするための「管理者用キーファイル」を作成します。

① [スタート] > [SecureDoc Enterprise Server] > [SecureDoc Enterprise Server]を実行します。

② 次の画面が表示されたら、<Create Key file>ボタンをクリックします。



③ 次の画面が表示されます。



<Browse> ボタンをクリックし、キーファイルを保存する場所と、ファイル名を指定します。

次のガイドに従って、必要事項を入力してください。拡張子は、「.dbk」です。

（例） C:¥SES¥seskey.dbk

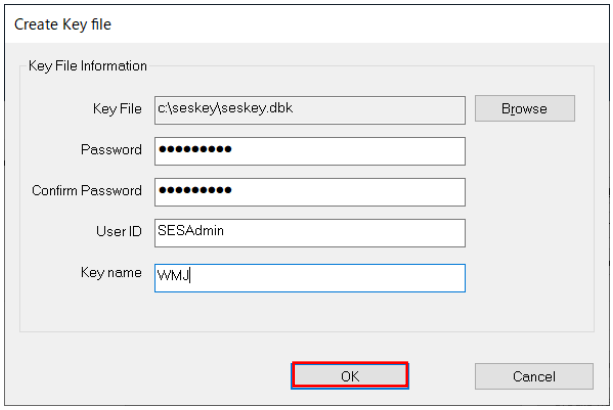
「Password」に強固なパスワードを入力し、「Confirm Password」に再度同じパスワードを入力してください。

「User ID」欄に、SES の管理者 ID 名を入力してください。

（例） SESAdmin

「Key Name」欄にデータベースを暗号化する鍵名を入力します。会社名の略称や「seskey」のようにデータベースの暗号鍵であることが分かる名前にします。

＜入力例＞

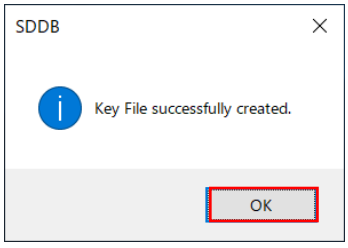


メモ：

Key File	
Password	
User ID	
Key name	

入力が完了したら、<OK>をクリックします。

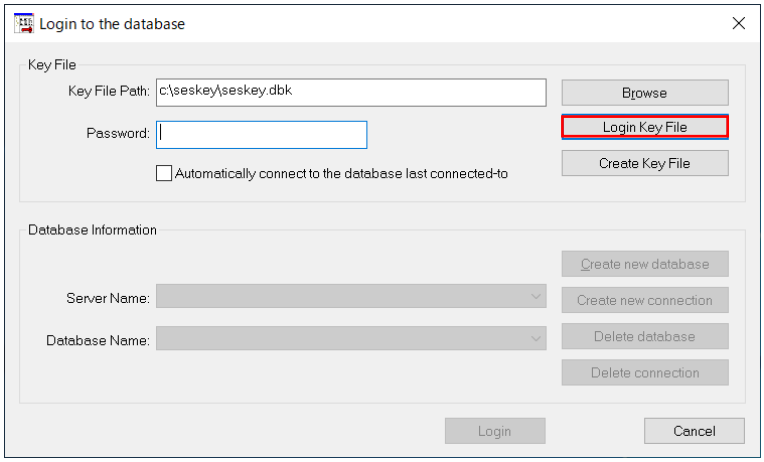
④　作成に成功すると、以下の画面が表示されます。<OK>をクリックします。



⑤　②の画面に戻ります。

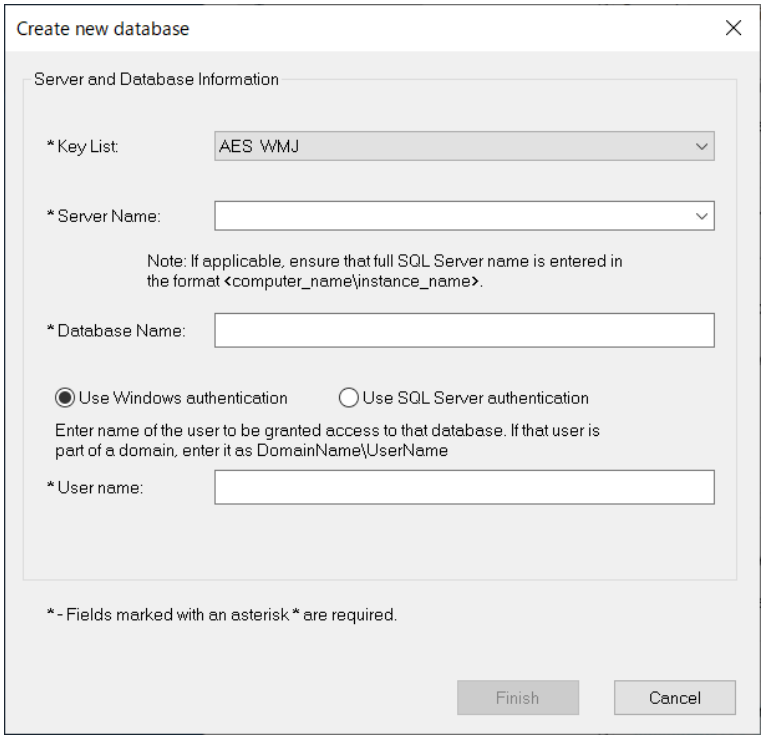
作成済のキーファイルを使って SES にログインし、SQL にデータベースを作成します。

先に設定したパスワードを入力し、<Login Key File>をクリックします。



ログインに成功すると、グレーアウトしていたメニューが表示されます。

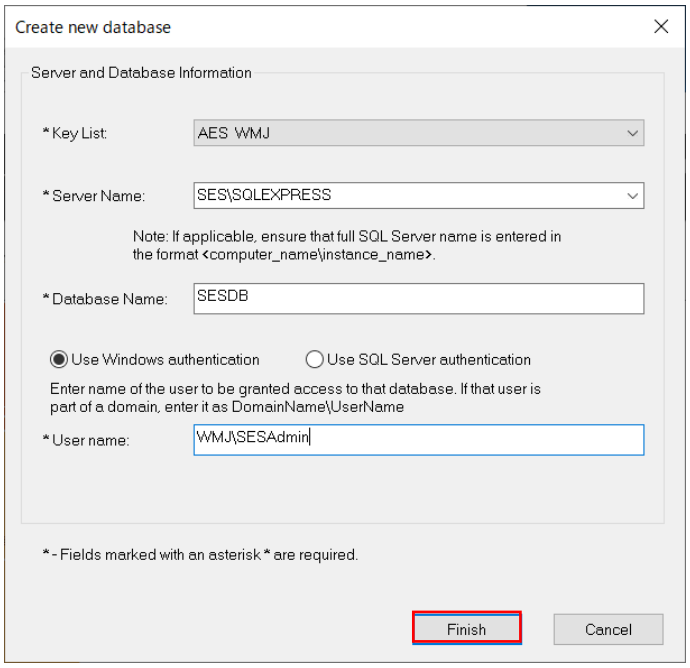
⑥ <Create new database>をクリックします。次の画面が表示されます。



⑦ 次のテーブルを参照して、必要な情報を入力します。

項　目	説　明
Key List	ドロップダウンから、データベースを暗号化する鍵を選択します。 SES で管理する DB が一つの場合、鍵は一つだけです。
Server Name	SQL サーバー名を「コンピューター名¥SQL インスタンス名」という形式で入力します。 SQL Express では、「コンピューター名¥SQLEXPRESS」と入力してください。
Database Name	任意のデータベース名を入力します。 SQL Server に、ここで入力した DB が作成されます。
Use Windows Authentication	SQL データベースへのログインに、Windows ログイン認証を利用します。 「ドメイン¥ユーザー」の形式で資格情報を入力します。 「User name」には、「6.1.SES で使用するアカウント」で説明した単一のアカウントを使用してください。 ローカル Administrator 権限が必要です。
Use SQL Server Authentication	SQL データベースへのログインに、SQL のシステム管理者のアカウント（sa）を利用する場合は、こちらを選択します。 SQL Login ID と「パスワードを設定します。

＜入力例＞



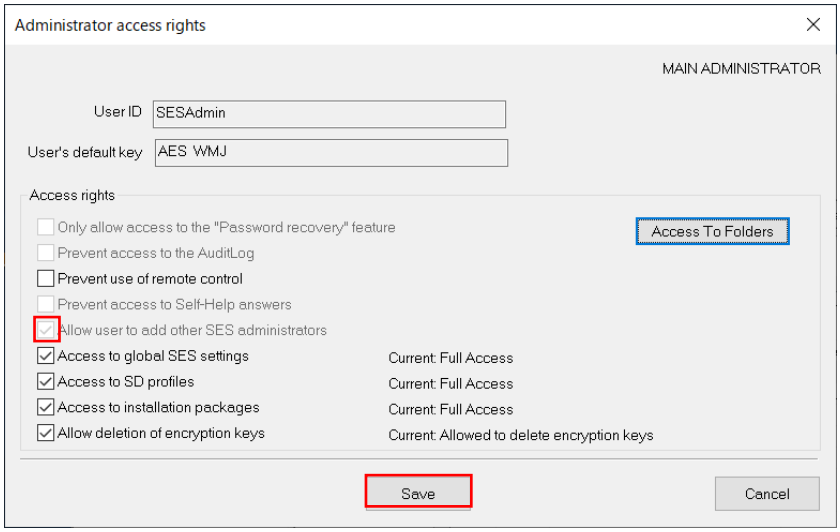
メモ：

Server Name	
Database Name	
Use Windows Authentication	ユーザー名：
Use SQL Server Authentication	SQL ログイン ID: パスワード：

⑧　入力を終えたら、<Finish>をクリックします。

⑨ DB の作成後、管理者の権限を設定する画面が表示されます。
最初のインストールでは、初めての管理者登録なので、すべての権限を与えなければなりません。
デフォルトで設定されている状態のまま（下図参照）で、<Save>をクリックします。

注 ここで作成する管理者に、SES コンソールで別の SES 管理者を作成し追加する許可をする場合は、[Allow user to add other SES administrators] にチェックを入れて、<Save>をクリックします。
パスワードリカバリーのみの権限を付与した管理者を作成する場合や、特定の組織のみの管理する管理者を作成する場合などを考慮してください。選択されなかった場合、後で SES 管理者を追加することはできません。



これで、管理者の作成とデータベースの作成が完了しました。SES コンソールが起動します。

注 最後に、管理者用のキーファイル（***.dbk）は、必ず安全な場所にバックアップしてください。
ここで作成したキーファイルを誤って削除、あるいはパスワードを失念すると、SES コンソールにログインできなくなります。

8.2. SES DB にアクセスするアカウントの設定

SDConnex、ADSync が SQL Server に作成した SES の DB に接続するための設定をおこないます。

「Account」で接続する場合、「6.1.SES で使用するアカウント」で説明した単一のアカウントを使用してください。

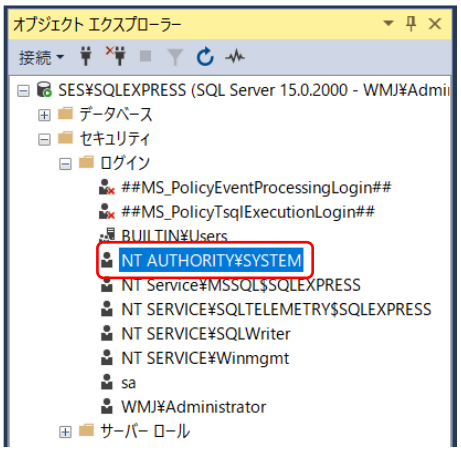
① SQL Server Management Studio を起動します。

② Windows 認証を選び、<接続>をクリックします。

1）SDConnex、ADSync で「Local System」を利用する場合、

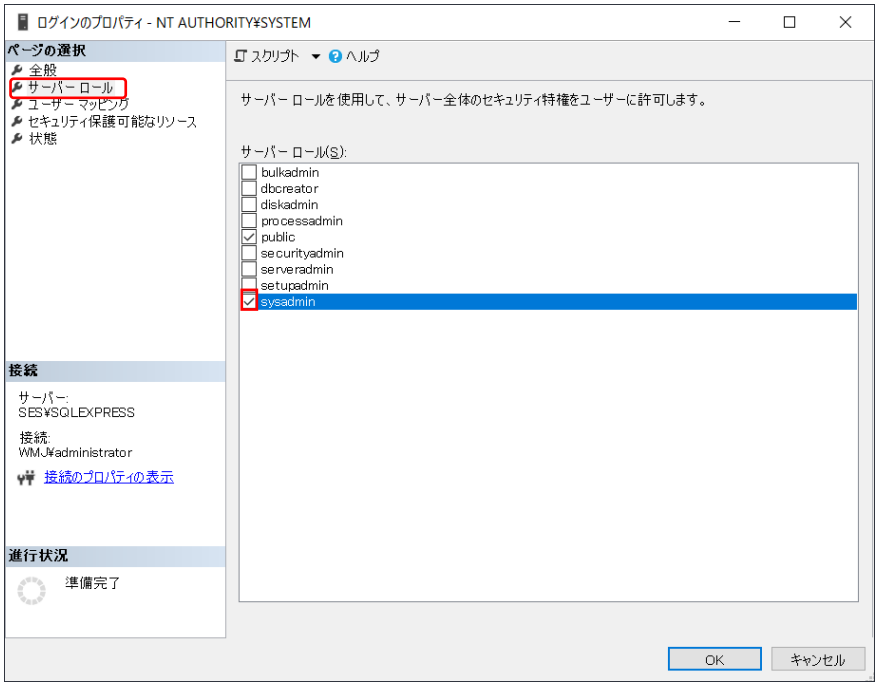
「Account」を利用する場合は、次章をご参照ください。

① オブジェクト エクスプローラーで、[セキュリティ] を展開し、[ログイン] から
[NT AUTHORITY¥SYSTEM] をダブルクリック、もしくは右クリックメニューで [プロパティ] を実行します。



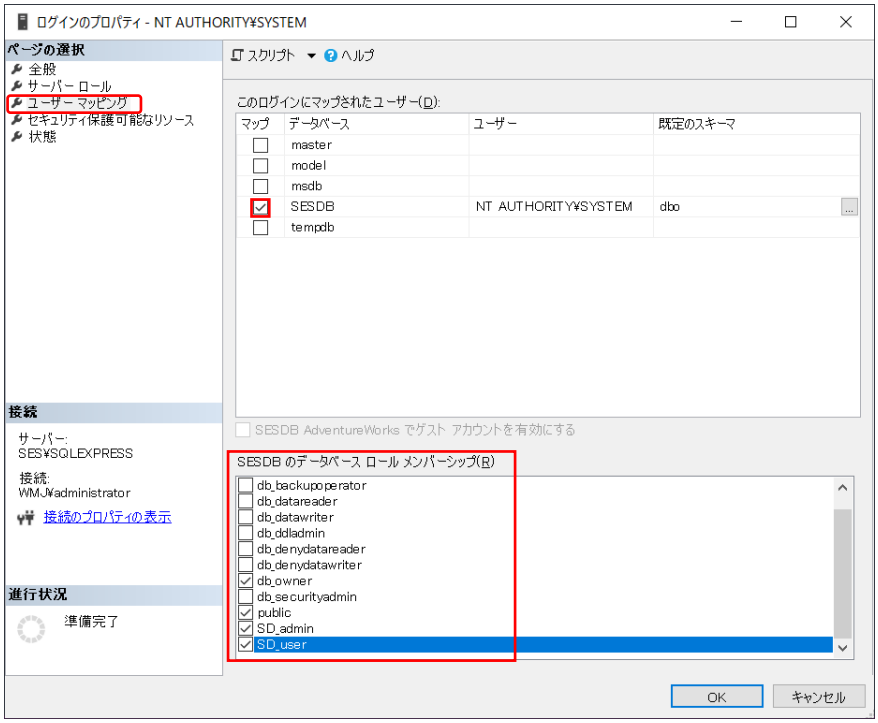
② [サーバーロール] をクリックします。

[Public] のみが選択されていますので、[sysadmin] にチェックを入れます。



③ 続けて、左ペインから [ユーザマッピング] をクリックし、データベースの一覧から先に作成した SES の DB にチェックを入れます。下記のロールメンバーを追加し、<OK>をクリックします。

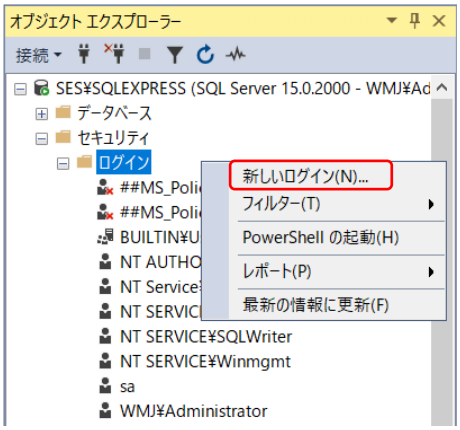
db_owner
SD_admin
SD_user



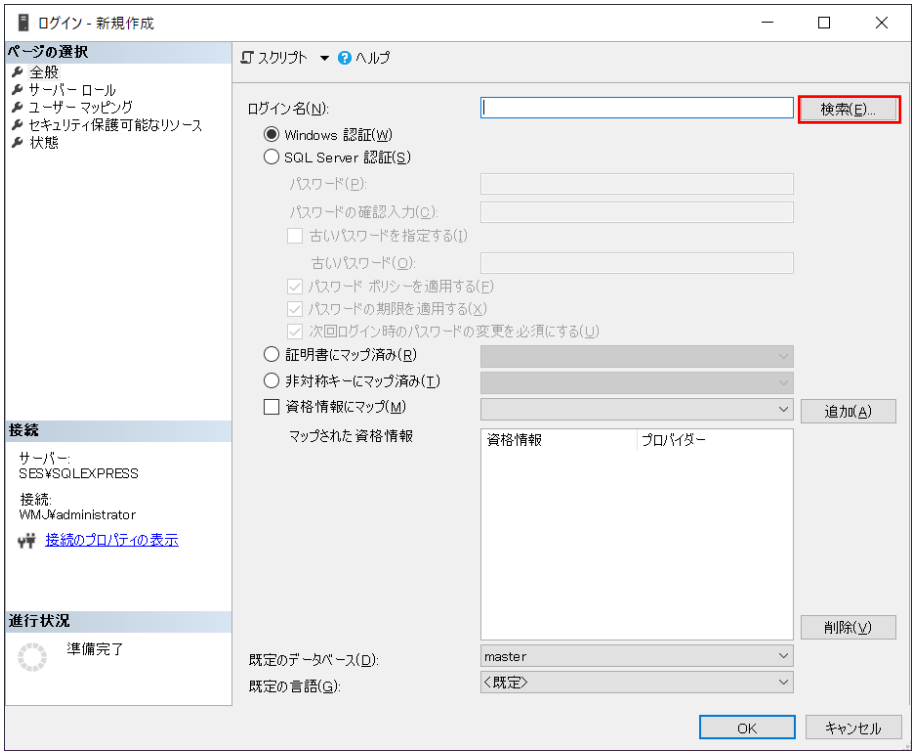
※ SES のデータベース名は、お客様毎に異なります。

2）SDConnex、ADSync で「Account」を利用する場合、

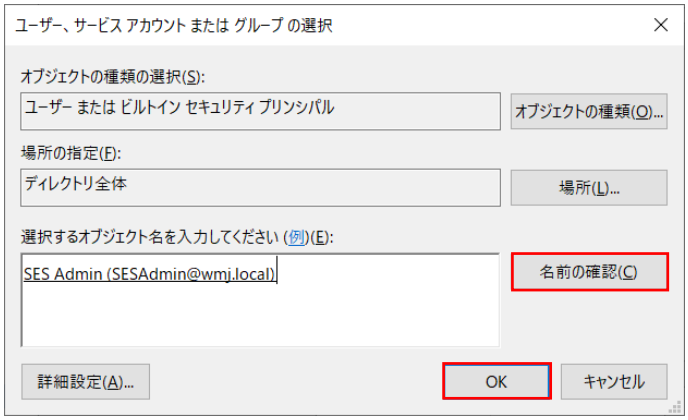
① オブジェクト エクスプローラーで、[セキュリティ] を展開し、[ログイン] を右クリックし、[新しいログイン] を実行します。



② 「ログイン名」欄で、<検索>をクリックし、SDConnex 等を起動するアカウントを選択します。

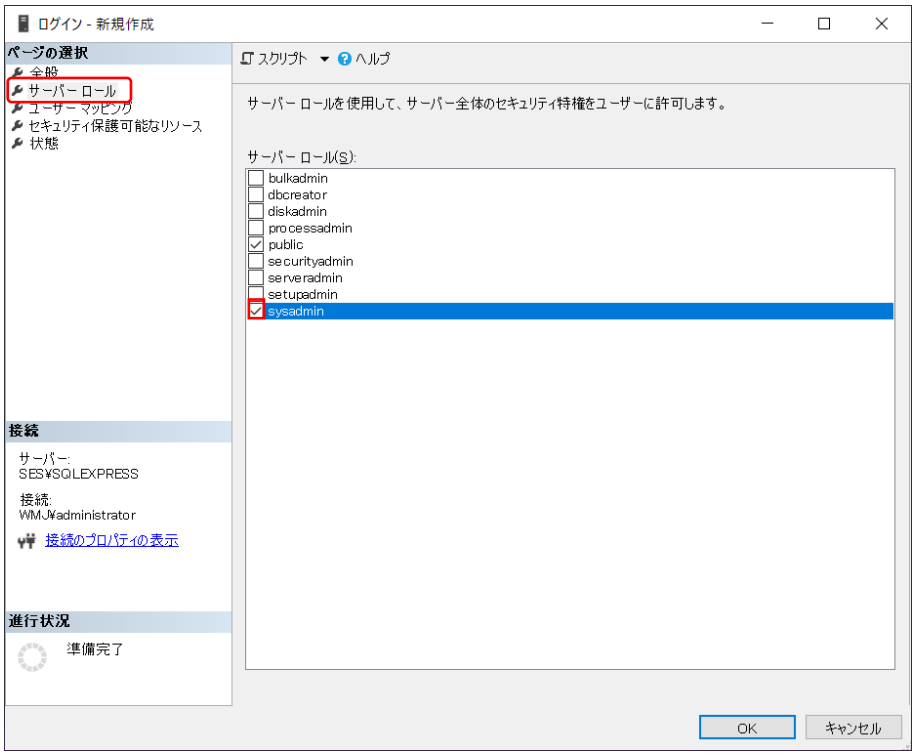


③ 「選択するオブジェクト名を入力してください」の欄で、アカウント名を入力し、<名前の確認>をクリックします。目的のアカウントを選択できたら、<OK>をクリックします。



④ 続けて、[サーバーロール] をクリックします。

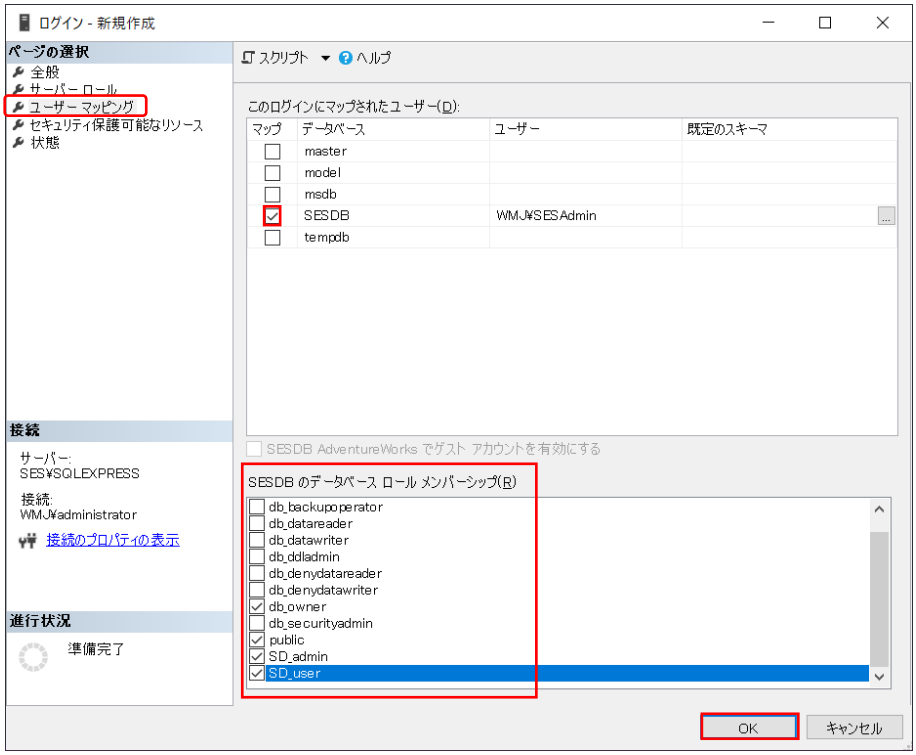
[Public] のみが選択されています。[sysadmin] にチェックを入れます。



⑤　続けて、左ペインから［ユーザマッピング］をクリックし、データベースの一覧から先に作成した SES の DB にチェックを入れます。

下記のロールメンバーを選択し、<OK>をクリックします。

db_owner
SD_admin
SD_user



※　SES のデータベース名は、お客様毎に異なります。

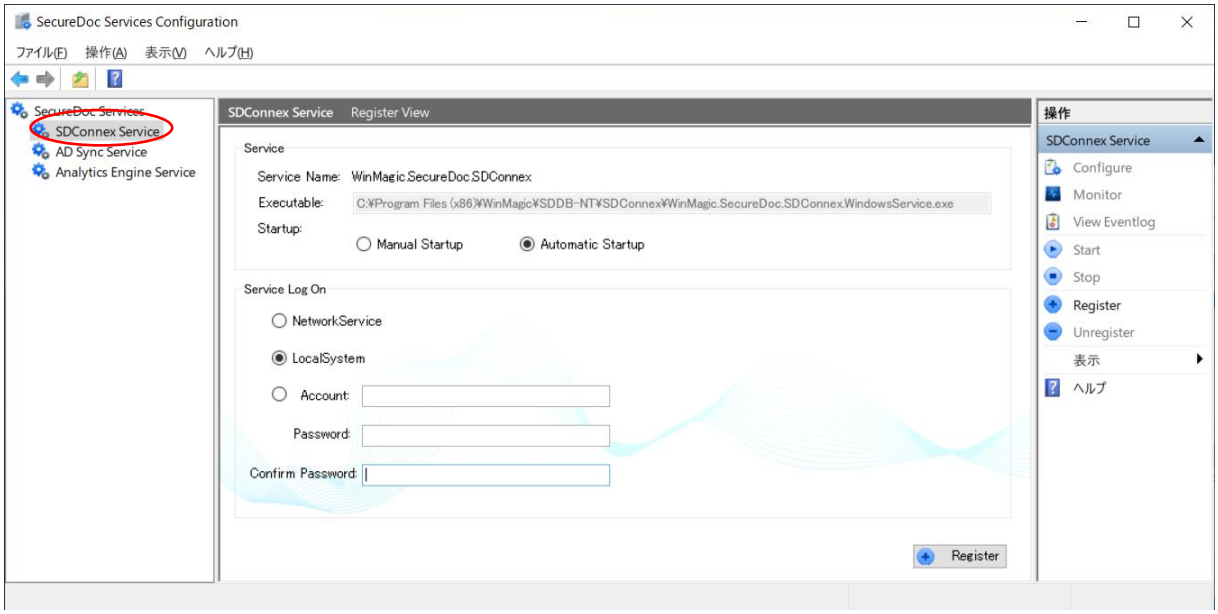
8.3. SDConnex サービスの開始

SDConnex を Windows のサービスとして起動するように設定します。

注　SQL Server がインストールされているサーバー以外に、SDConnex、ADSync をインストールする場合 SQL Express のデフォルト設定では、インストールされているサーバーと同じサーバーからの接続のみを許可しますので、そのままでは SDConnex は SQL に接続することができません。SQL Server 構成マネージャーを使ってプロトコルの設定、ポートの設定、SQL Server Browser 等の設定が必要です。
詳しくは、マイクロソフト社のサイトをご参照ください。
https://docs.microsoft.com/ja-jp/sql/relational-databases/lesson-2-connecting-from-another-computer?view=sql-server-ver16

① [スタート] > [SecureDoc Enterprise Server] > [SecureDoc Services Configuration]を実行します。

② 左ペインから、[SDConnex Service] を選び、右ペインの操作メニューにある [Register]をクリックします。
「SDConnex Service Register View」画面が表示されます。

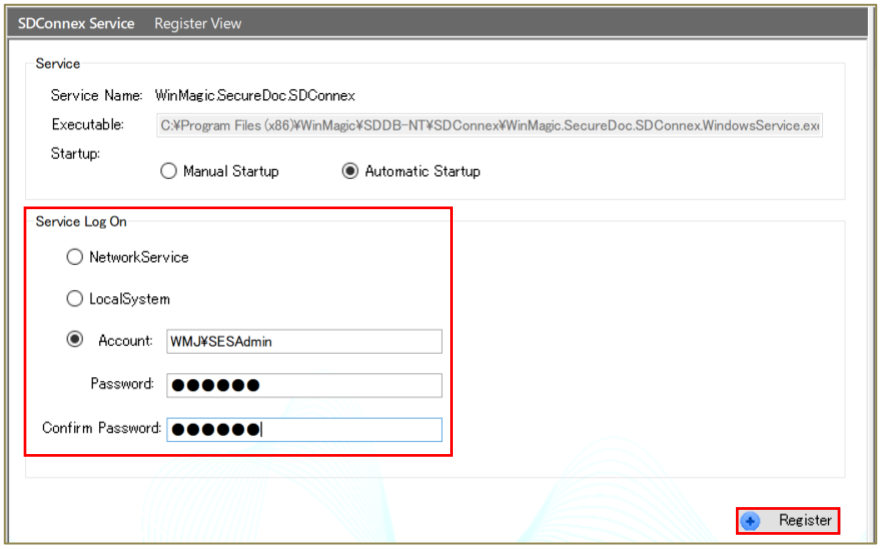


③ 「Service」の枠で、SDConnex のサービス起動に関する設定をします。
特別な理由がない限り、そのまま [Automatic Startup] を選択し、Windows 起動時に SDConnex が自動で開始するようにします。手動で開始する場合は、[Manual Setup] を選択します。

「Service Log On」の枠では、サービスを起動するアカウントを設定します。

※　サービスを起動するアカウントは、お客様の企業ポリシーあるいは環境にあわせて選択することができます。デフォルト設定は 「Local System」です。「Account」で設定する場合、「6.1.SES で使用するアカウント」で説明した単一のアカウントを使用してください。「ドメイン¥ユーザー」の形式で資格情報を入力します。

設定例： Account 設定

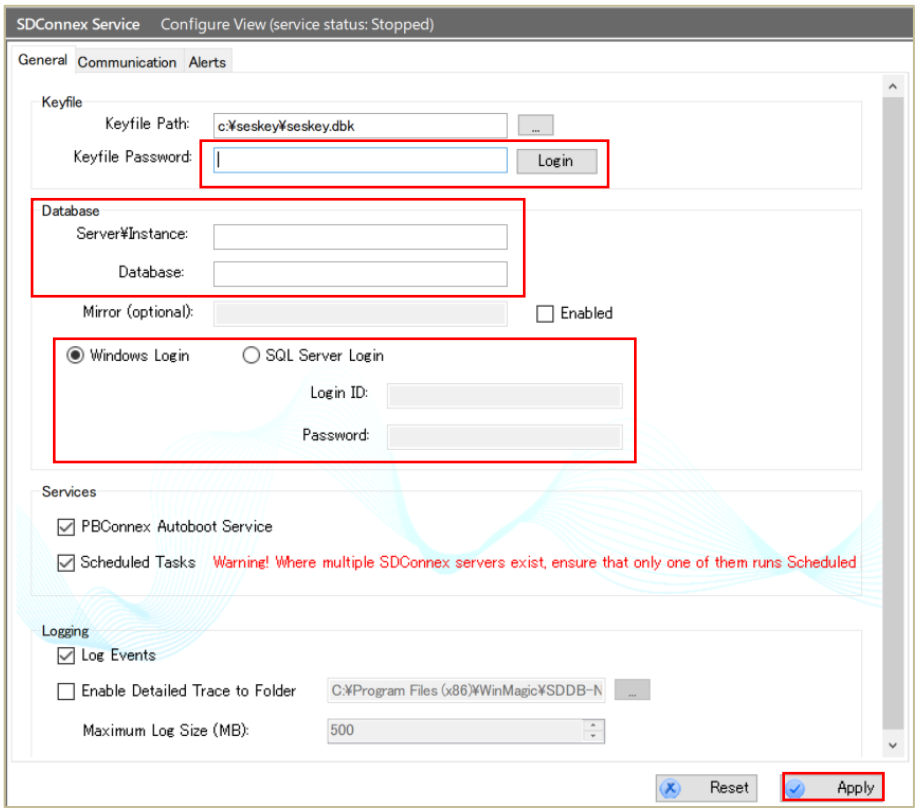


※ Web コンソールを利用する場合は、IIS の設定で、アプリケーションプール ID に、ここで登録した資格情報と同じものを設定します。

④ 右下にある<Register>をクリックすると、Windows のサービスとして登録されます。

⑤ 「SDConnex Service」画面に、3 つの設定タブが表示されます。

⑥ 「General」タブでは、SES DB への接続を設定します。



⑦ 「Keyfile Path:」では、「8.1.1 管理者用キーファイルとデータベースの作成」で、作成した管理者用キーファイルのファイル名を指定します。（通常は自動で入力されます。）

「Keyfile Password:」で、キーファイルのパスワードを入力し、<Login>をクリックします。

正しいパスワードが入力されると、「Server ¥ Instance」、「Database」の情報が自動的に入力されます。

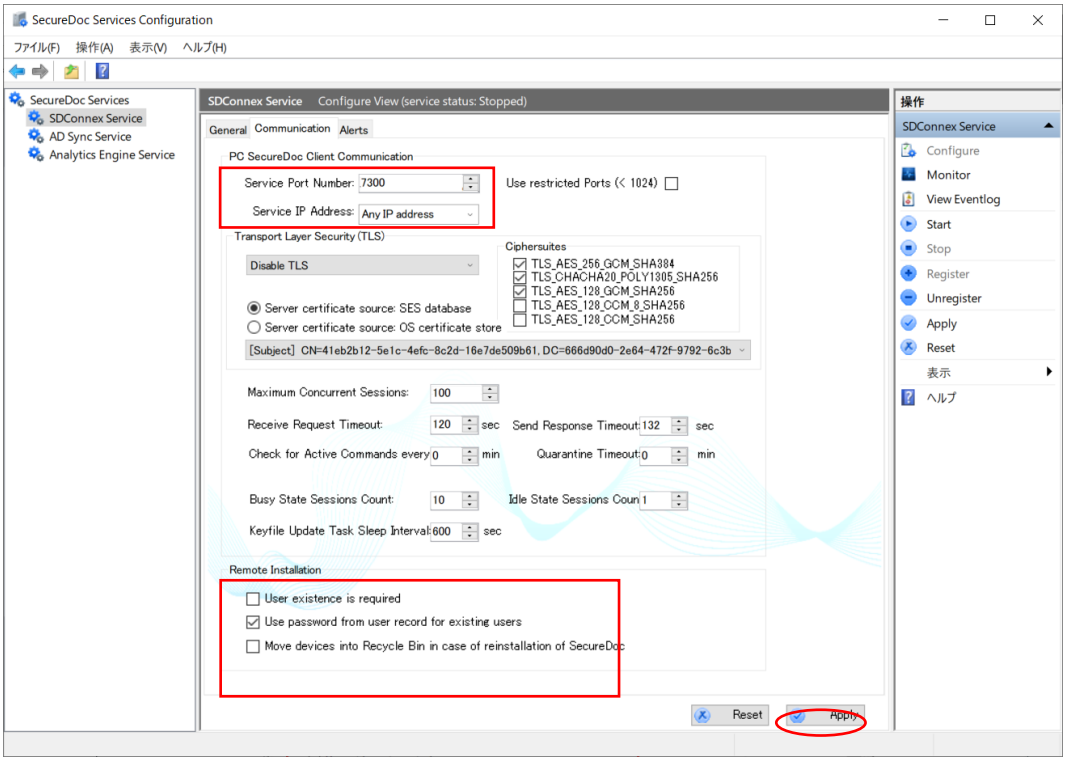
次に、SQL DB にアクセスするための認証方法を設定します。通常は、Windows 認証モードで SQL に接続する [◎Windows Login] を選択します。

General

項　目	説　明
Keyfile	
Keyfile path:	キーファイルを指定します。
Keyfile Password:	キーファイルのパスワードを入力します。
Database	
Server¥Instance:	SQL のインストールされているサーバー名とインスタンスを指定します。
Database:	接続するデータベース名を入力します。
◎ Windows Login	Windows 認証モードで、SQL に接続します。
○ SQL Server Login	SQL Server 認証モードで、SQL に接続します。

⑧ [Communication]タブをクリックします。

次の画面が表示されます。



「Service Port Number:」は、SDConnex が SecureDoc クライアントと通信に使用するポート番号の設定で、デフォルト設定は「7300」です。社内ネットワーク環境で、このポート番号が使用できない場合は、他のポート番号に変更します。

「Service IP Address:」では、SDConnex を実行するサーバーの IP アドレスを設定します。

注　IP アドレスは、通常、[Any IP address] のままで構いませんが、複数の NIC が装着されているハードウェア環境の場合や、仮想環境にインストールした場合は、[Any IP address] ではなく、プルダウンメニューで表示された IP から適切なものを選んでください。

⑨　必要に応じて、「Remote Installation」の設定を変更できます。次のテーブルを参照してください。

設定は、いつでも変更できます。

他の項目は通常デフォルト設定のままで使用します。

ウィンマジックのサポートから指示があった場合以外は、設定変更をする必要はありません。

Communication

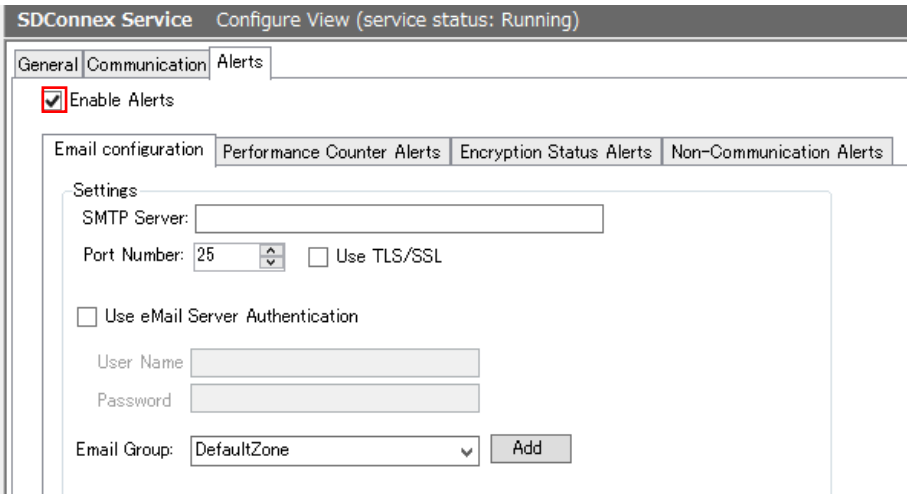
項　目	説　明
PC SecureDoc Client Communication	
Service Port Number:	SecureDoc クライアントと SDConnex が通信に使用するポート番号
Use restricted Ports(<1024)☐	1024 以下のポート番号を使用する場合
Service IP Address:	SDConnex のサービスを起動するサーバーの IP アドレス
Transport Layer Security (TLS)	
Disable TLS（デフォルト設定）	HTTPS あるいは TLS を使用する場合、下記の選択肢から選択します。 Use HTTPS or TLS 1.3 where Supported Force use of TLS 1.3 Force use of HTTPS Ciphersuites から TLS 暗号スイートを選択します。
◎ Server certificate source SES database ○ Server certificate source OS certificate store SES データベースをソースとするサーバー証明書以外に、OS 証明書ストアで発行した証明書を設定できます。	
Maximum Concurrent Sessions:	最大同時セッション数 デフォルト値：100
Receive Request Timeout:	受信リクエストのタイムアウト デフォルト値：120 sec
Send Response Timeout:	応答送信のタイムアウト デフォルト値：120 sec
Check for Active Command every:	アクティブなコマンドをチェックする間隔 デフォルト値：120 min

項　目	説　明
Quarantine Timeout:	隔離タイムアウト デフォルト値：0 min
Busy State Session Count:	ビジー状態のセッション数
Idle State Session Count:	アイドル状態のセッション数
Keyfile Update Task Sleep Interval:	キーファイル更新タスクのスリープ間隔
Remote Installation	
☐ User existence is required	SES DB に存在するユーザーのみにインストールを許可します。 AD Sync や CSV で SES にインポートした ID と、一致した Windows サインイン名のクライアントのみに SecureDoc のインストールを許可することができます。 クライアントインストール実行時に、SES DB にユーザーが存在しない場合、インストールは許可されず中止されます。 これにより、意図しない ID が作成されるのを防げます。
☑ Use password from user record for existing users	キーファイルのイニシャルパスワードとして、SES DB のユーザーに記録されたパスワードを使用する場合、オンにします。SES からユーザーをクライアントに配信する際等に使われます。
☐ Move devices into Recycle Bin in case of reinstallation of SecureDoc	SecureDoc がクライアント デバイスに再インストールされた場合、SES に既に存在するデバイスを Recycle Bin に移動します。 これにより、SES DB でデバイスが重複するのを防ぎます。

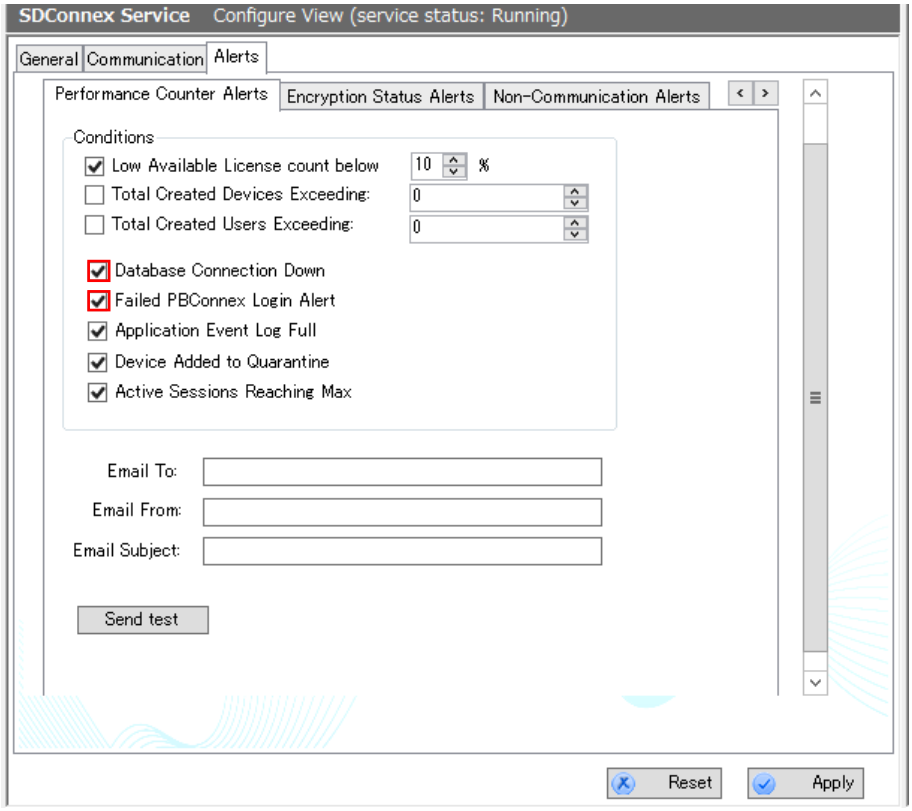
⑩　設定後、右下にある<Apply>をクリックします。

⑪　SDConnex が、SES DB との接続に問題が発生した場合等、電子メールで通知する場合は、[Alerts] タブをクリックします。この設定は、必須ではありません。設定はいつでも可能です。次の画面が表示されます。

[Enable Alerts] のチェックボックスをオンにし、メールの設定をします。



⑫ SES DB へのアクセス問題発生時に、アラートを通知する場合は、[Performance Counter Alerts] のタブをクリックします。[Database Connection down] にチェックを入れます。
プリブートネットワーク認証を使用する環境では、[Failed PBConnex Login Alert] にチェックを入れます。

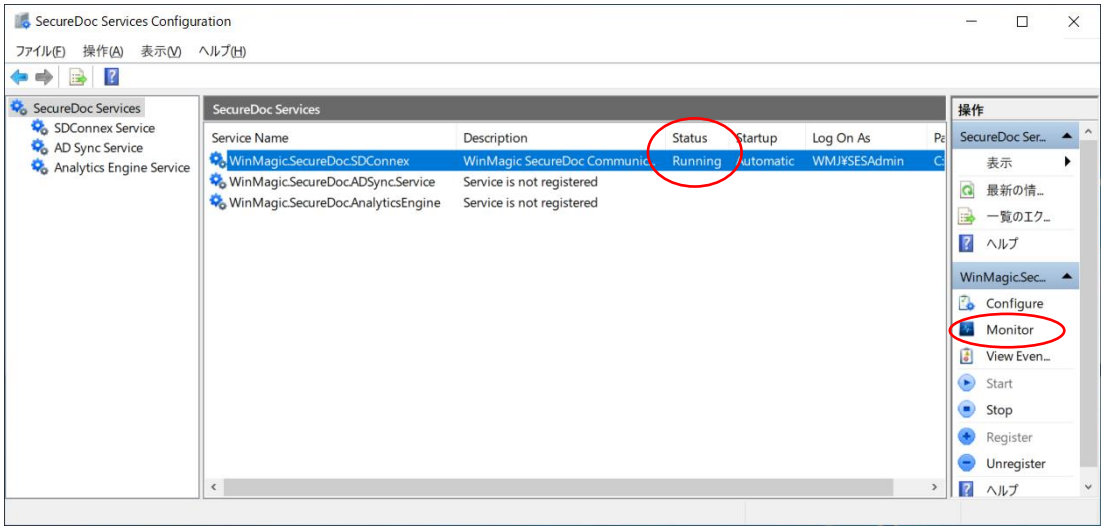


電子メールの宛先と差出人、件名を入力します。<Send test>をクリックし、送信テストが可能です。

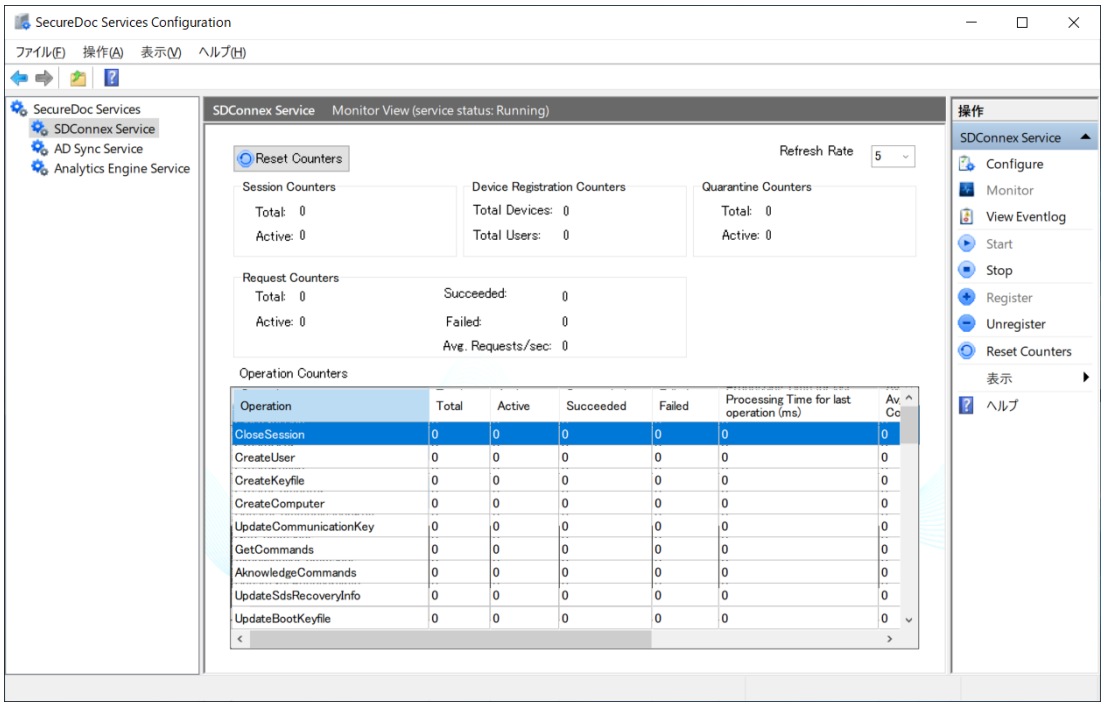
⑬ 設定後、右下にある<Apply>をクリックします。

⑭ 必要な設定が完了したら、右ペインにある[Start] をクリックします。

⑮ 次のように、[Status] が、Running になっていることを確認してください。
SDConnex のサービスが起動したら、右ペインの [Monitor] をクリックします。



⑯ 次の画面が表示され、SecureDoc クライアントのインストール時やクライアントが SDConnex と通信すると、Session Counters の数がカウントアップされます。



⑰ SDConnex の設定は、これで完了です。

8.4. Microsoft Active Directory との連携

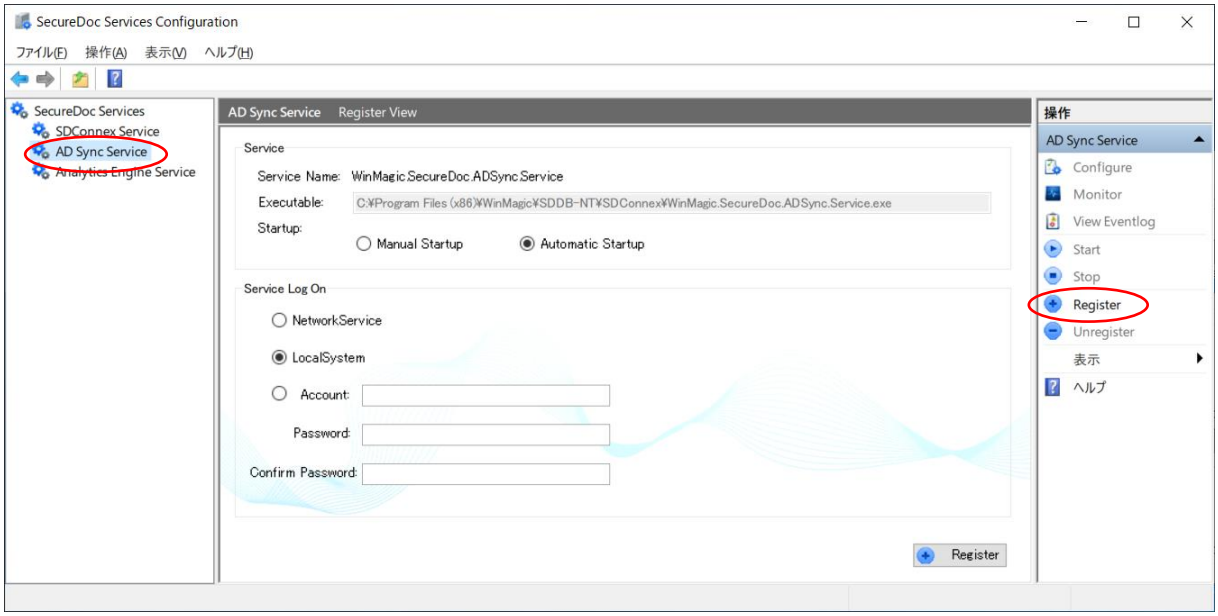
Active Directory（以下、AD）と連携すると、OU（フォルダ）に含まれるユーザー情報とグループを AD と同期できます。

※　AD と同期しない場合、設定をおこなう必要はありませんので、スキップしてください。
導入前の評価テストの場合等では、必ずしも必要ではありません。

※　SES コンドメインメンバーであり、ドメインユーザーにてログインしていることを確認します。
SES コンソールでのユーザー追加や削除などの操作は、AD 側に同期されません。

①　[スタート] > [SecureDoc Enterprise Server] > [SecureDoc Services Configuration]を実行します。

②　左ペインから、[ADSync Service] を選び、右ペインの操作メニューにある [Register] をクリックします。
「ADSync Service Register View」画面が表示されます。

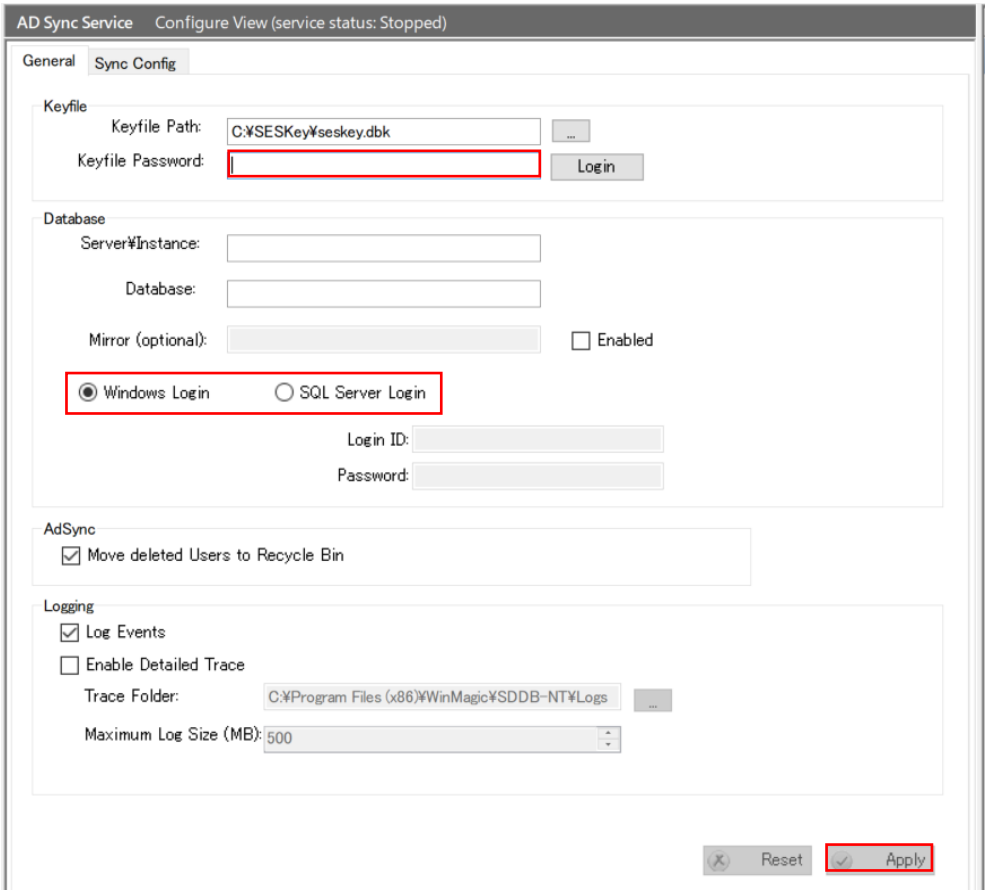


「Service」の設定は、通常、そのまま [Automatic Startup] を選択します。
「Service Log On」の枠は、ADSync サービスを起動するアカウントで、SDConnex と同じように設定します。
右下にある<Register>をクリックすると、Windows のサービスとして登録されます。

※　サービスを起動するアカウントは、お客様の企業ポリシーあるいは環境にあわせて選択することができます。
デフォルト設定は 「Local System」です。「Account」で設定する場合、「6.1.SES で使用するアカウント」で説明した単一のアカウントを使用してください。「ドメイン¥ユーザー」の形式で資格情報を入力します。

③ 「ADSync Service」画面に、2 つの設定タブが表示されます。

[General] タブでは、 SDConnex と同じように設定してください。



「Keyfile Path:」では、「8.1.1 管理者用キーファイルとデータベースの作成」で、作成した管理者用キーファイルのファイル名を指定します。（通常は自動で入力されます。）

「Keyfile Password:」で、キーファイルのパスワードを入力し、<Login>をクリックします。

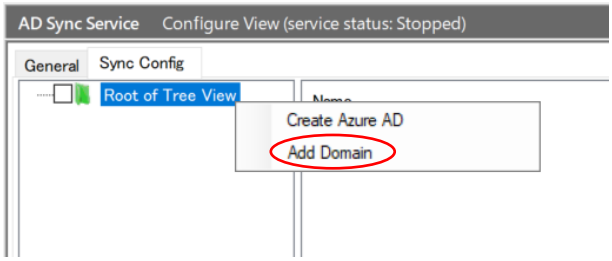
正しいパスワードが入力されると、「Server ¥ Instance」、「Database」の情報が自動的に入力されます。

次に、SQL DB にアクセスするための認証方法を設定します。通常は、Windows 認証モードで SQL に接続する [◎Windows Login] を選択します。

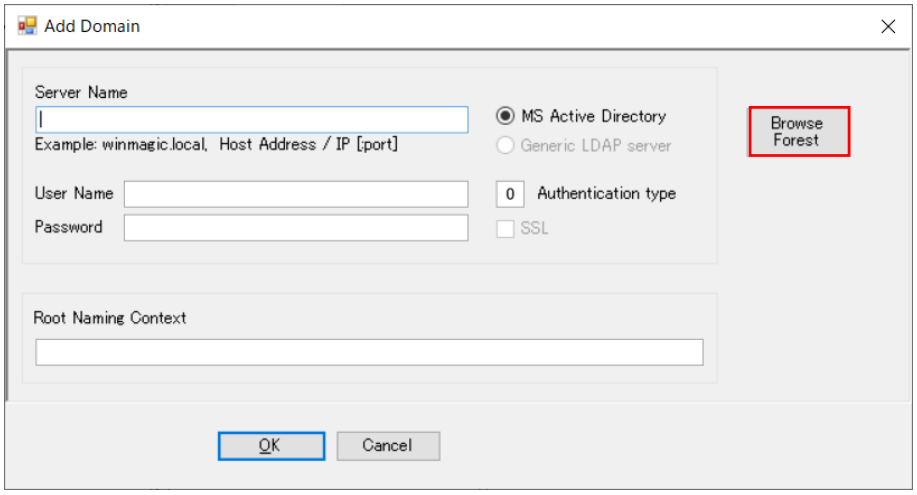
最後に、<Apply>をクリックします。

④ [Sync Config] タブをクリックします。

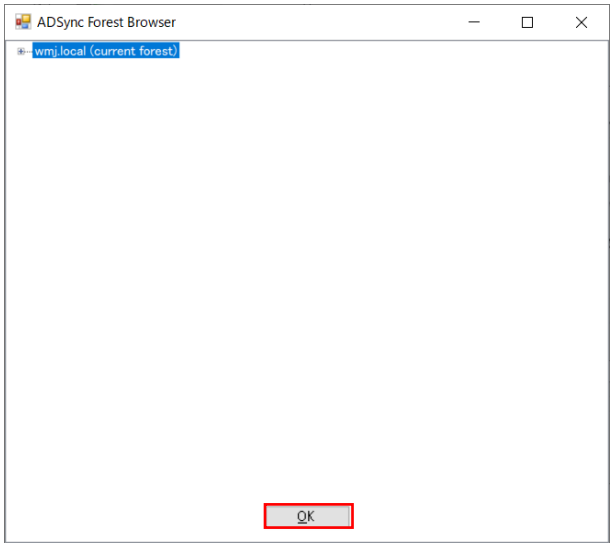
⑤　続いて、[Root of Tree View] のチェックボックスを右クリックし、[Add Domain]をクリックします。



⑥　次の画面が表示されます。<Browse Forest>ボタンをクリックします。



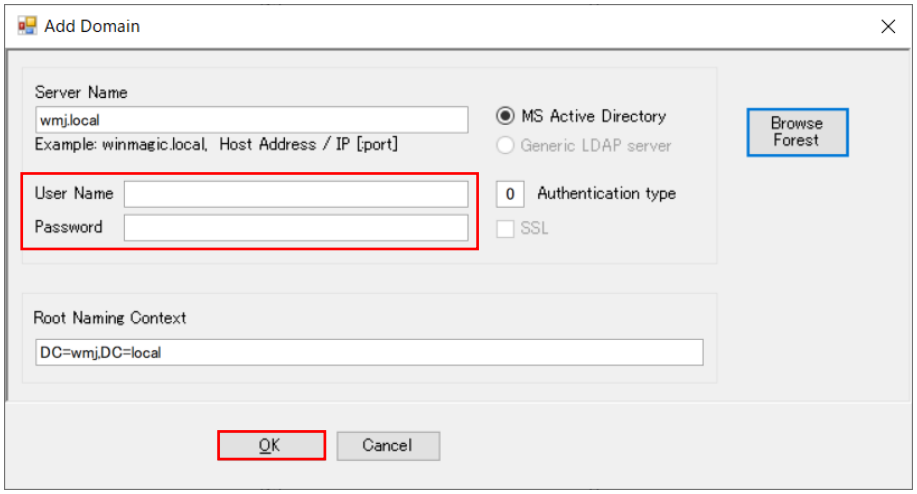
⑦　次の画面が表示されます。SES にインポートしたいドメインを選択し、<OK>をクリックします。



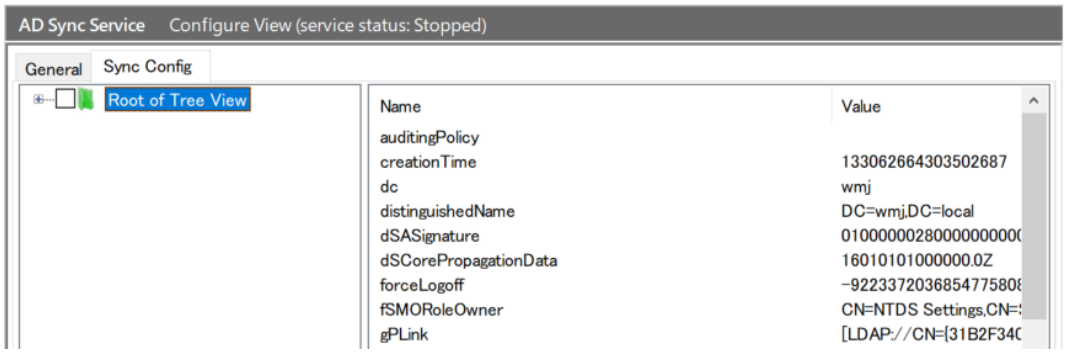
⑧ 前の画面に戻ります。

[Server Name] 欄と、[Root Naming Context] 欄が自動で入力されます。

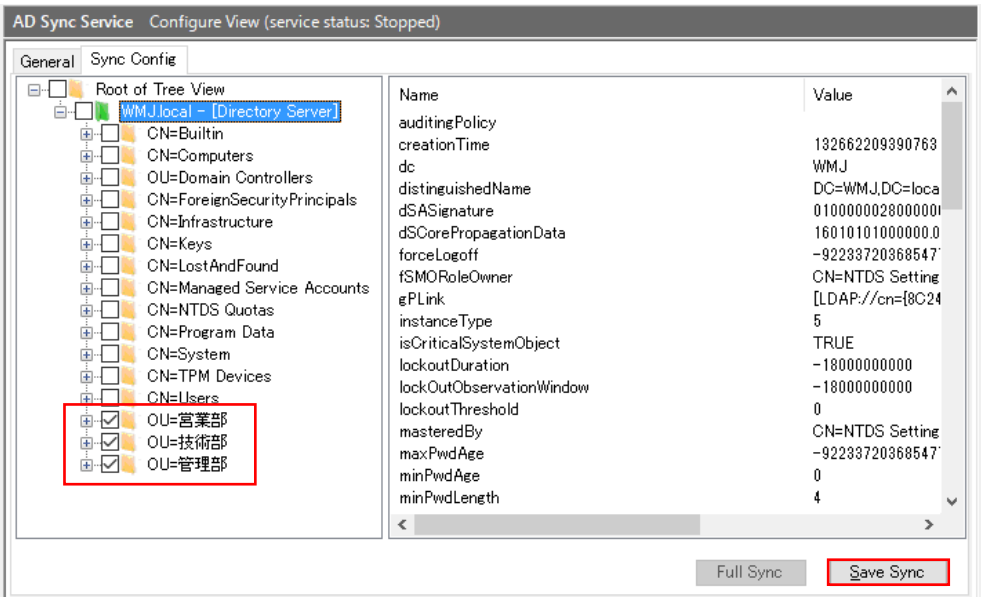
[User name] 欄にドメインユーザー名、[Password] 欄にパスワードを入力し、<OK >ボタンをクリックします



⑨ 次の画面が表示されたら、ツリーを展開します。

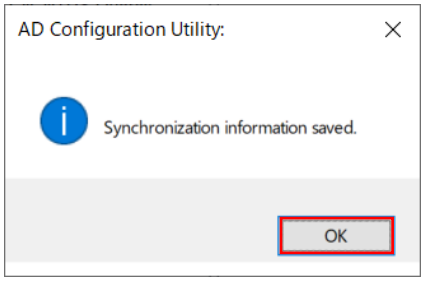


インポートする OU を選択し、<Save Sync>をクリックします。



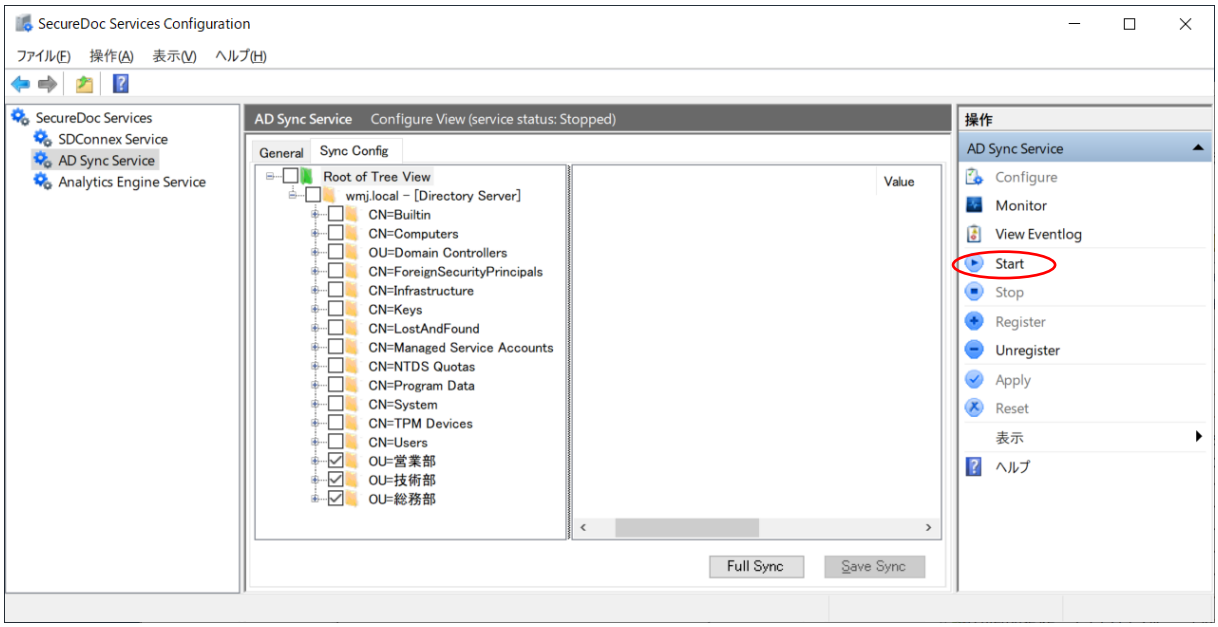
※　OU を展開すると、配下のユーザーを個々に選択することもできます

⑩　「Synchronization information saved.」というメッセージが表示されます。<OK>ボタンをクリックします。

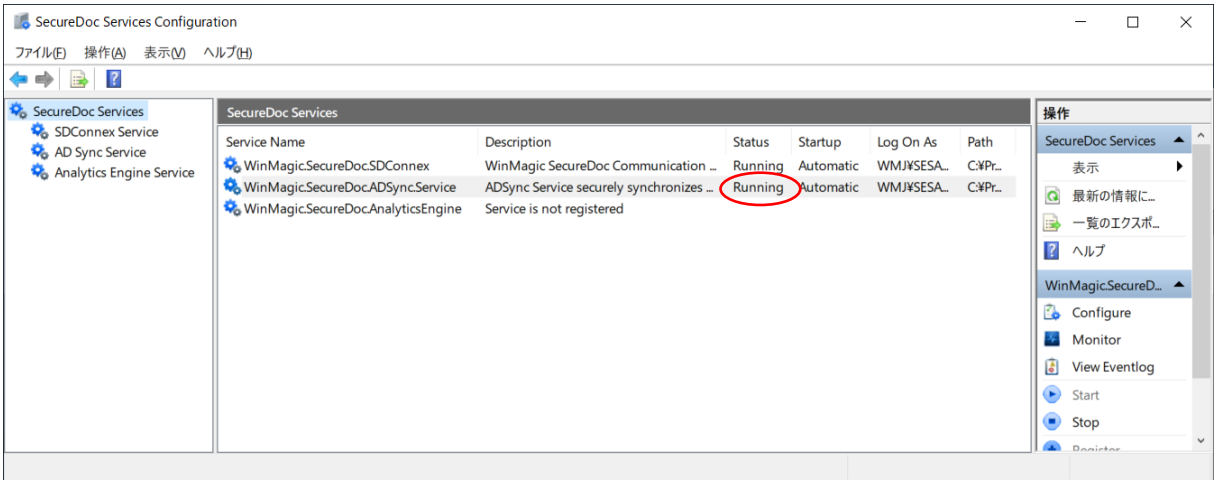


注　初回の同期時には、多くの時間を要する場合があります。

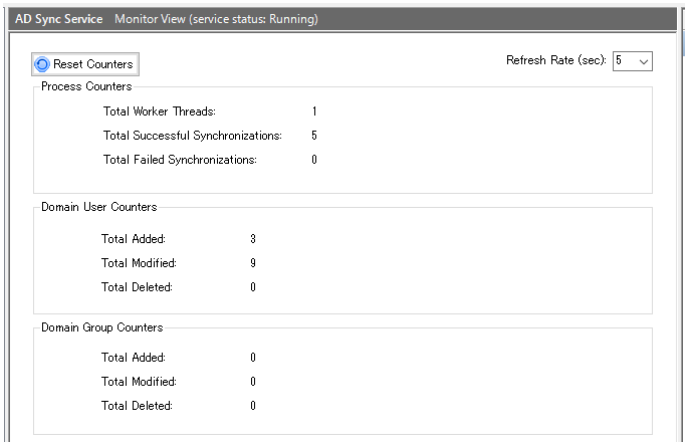
⑪　右ペインの操作メニューにある[Start] をクリックします。



⑫　トップ画面に戻ります。ADSync のサービスが Running になっていることを確認します。

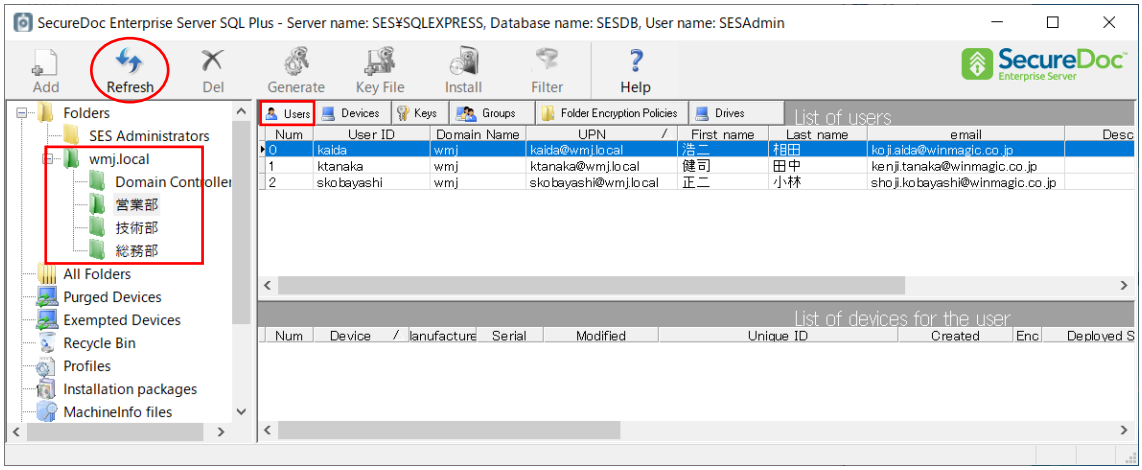


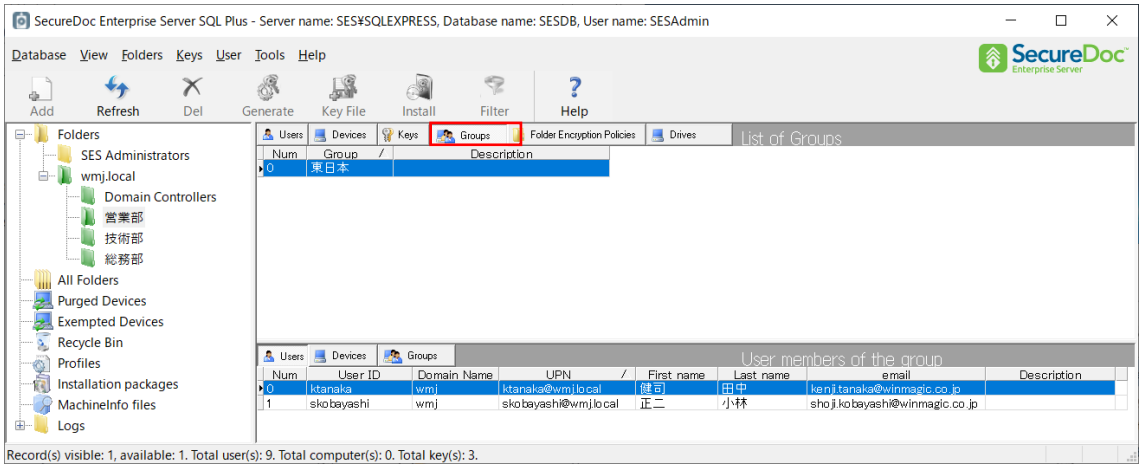
⑬ 右ペインの操作メニューにある[Monitor] をクリックすると、成功した同期の回数や SES に追加されたユーザー数等が表示されます。



⑭ ADSync による設定が完了すると、選択した OU とユーザー、グループが SES に追加されます。
SES を起動し、左ペインに緑色のフォルダが追加されていることを確認します。

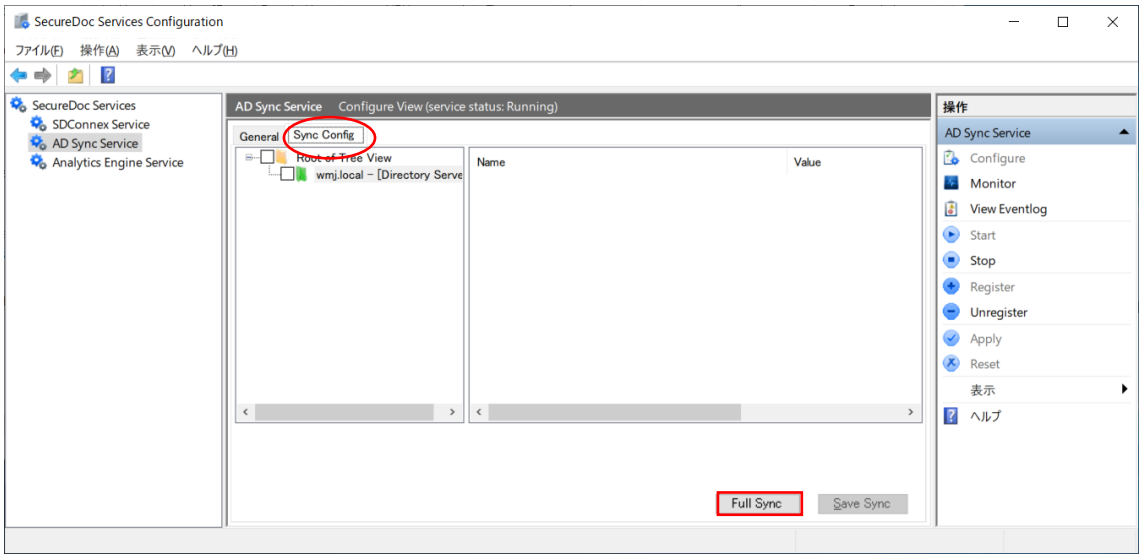
※ ADSync 設定前に、既に SES を起動していた場合は、<Refresh>ボタンをクリックして表示されている画面を更新してください。



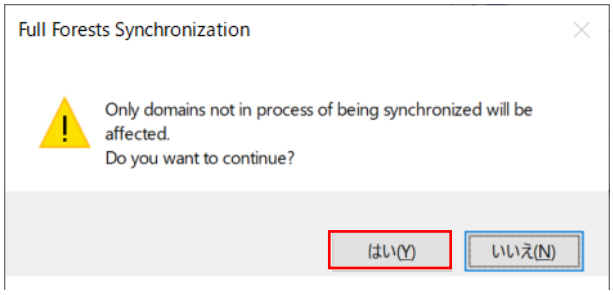


※ 完全同期は、ADSync のサービス起動時におこなわれます。その後は、変更のみを更新する部分同期が 1 時間毎におこなわれます。

SES コンソールにすぐに反映されない場合、あるいは変更をすぐに SES に反映させたい場合は、[Sync Config] タブを選び、<Full Sync>ボタンをクリックします。

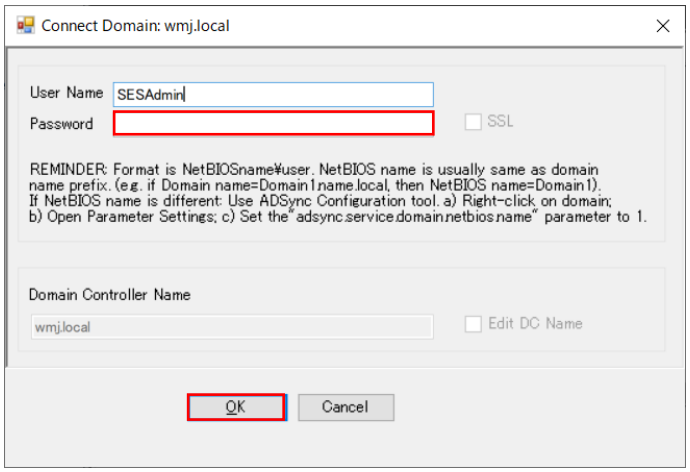


同期中でないドメインのみが影響を受けるという下記のアラートが表示された場合、<はい>をクリックします。

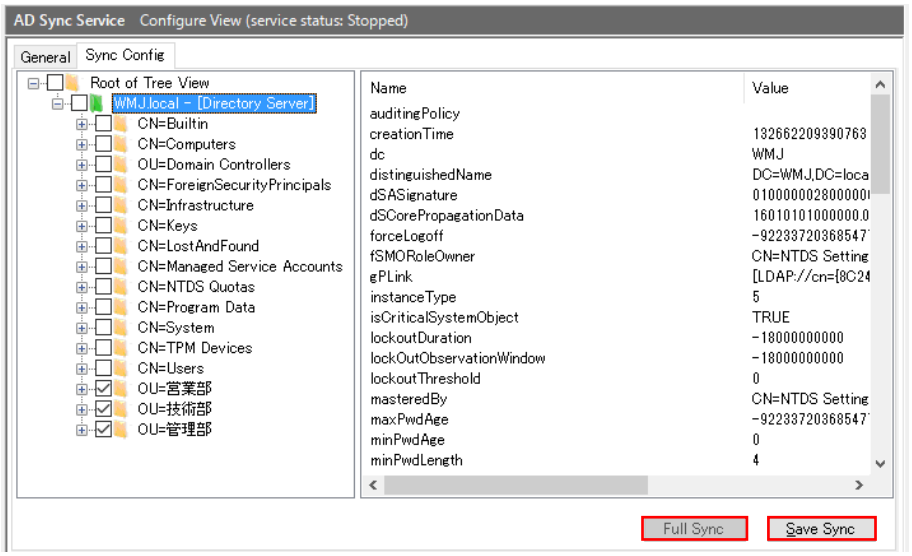


これまで指定されていない OU を新たに選択する場合は、ドメインのチェックボックスをクリックします。

ドメインへの接続画面が表示されるので、パスワードを入力し、<OK>をクリックします。



[Sync Config] タブを選び、同期したい OU のチェックボックスをオンにし、<Save Sync >をクリック後、<Full Sync>をクリックします。



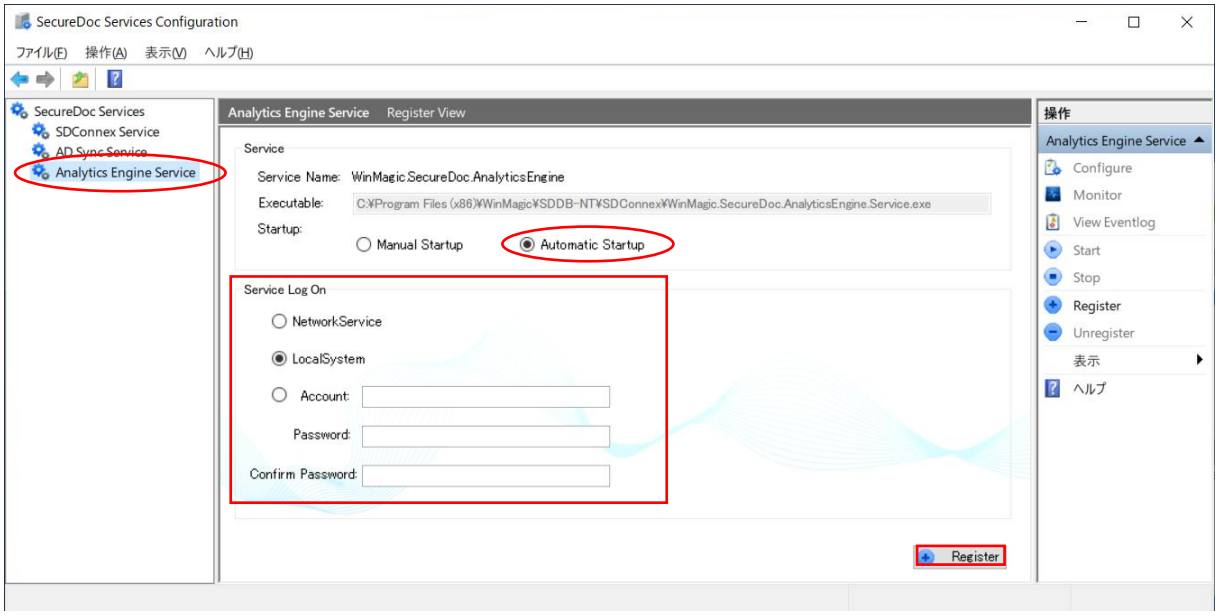
8.5. Analytics Engine の設定

SES Web コンソールを使用する場合、Analytics Engine の設定をします。

Analytics Engine Service は、SES v8.5 で追加された機能で、SES Web の System に表示する分析値のために必要です。

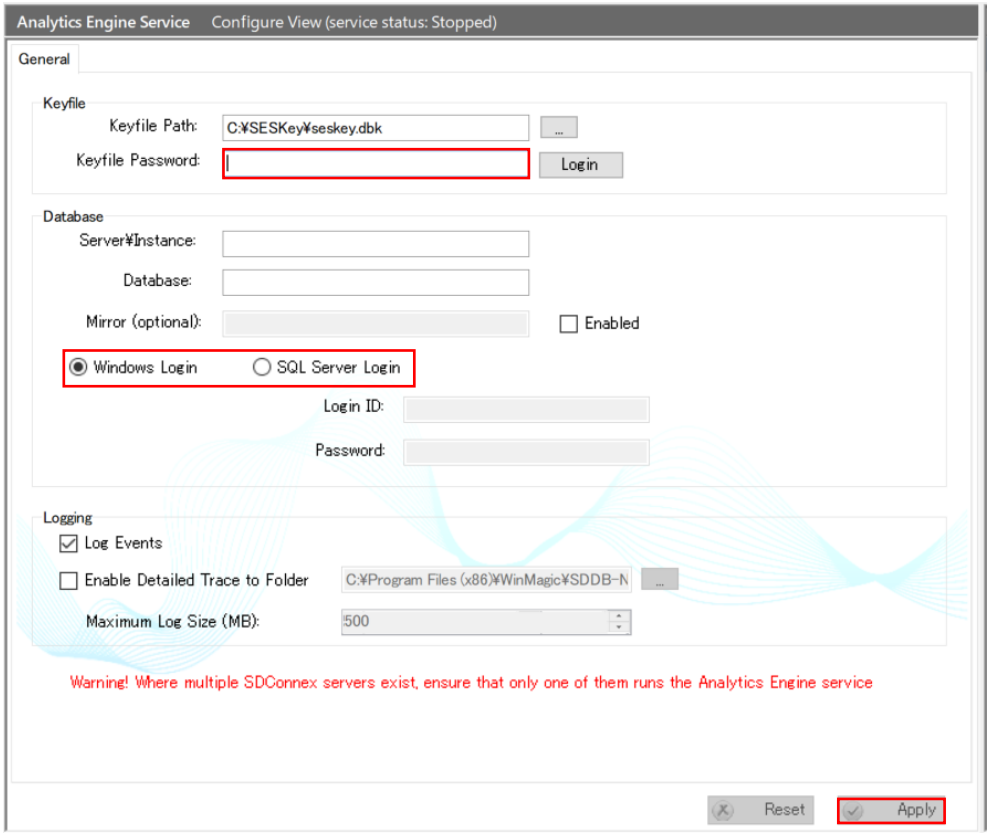
① [スタート] > [SecureDoc Enteprise Server] > [SecureDoc Services Configuration]を実行します。

② 左ペインより、< Analytics Engine Service >を選択します。
[Analytics Engine Service Register View] 画面が表示されます。



③ 「Service」の設定は、通常、そのまま [Automatic Startup] を選択します。
「Service Log On」の枠は、Analytics Engine サービスを起動するアカウントで、SDConnex と同じように設定します。
右下にある<Register>をクリックすると、Windows のサービスとして登録されます。
サービスを起動するアカウントは、お客様の企業ポリシーあるいは環境にあわせて選択することができます。
デフォルト設定は 「Local System」です。「Account」で設定する場合、「6.1.SES で使用するアカウント」で説明した単一のアカウントを使用してください。「ドメイン¥ユーザー」の形式で資格情報を入力します。

④ 「Analytics Engine Service」の [General] タブでは、 SDConnex と同じように設定してください



⑤ 「Keyfile Path:」では、「8.1.1 管理者用キーファイルとデータベースの作成」で、作成した管理者用キーファイルのファイル名を指定します。（通常は自動で入力されます。）

「Keyfile Password:」で、キーファイルのパスワードを入力し、<Login> をクリックします。

正しいパスワードが入力されると、「Server ¥ Instance」、「Database」の情報が自動的に入力されます。

次に、SQL DB にアクセスするための認証方法を設定します。通常は、Windows 認証モードで SQL に接続する [◎Windows Login] を選択します。

最後に、<Apply> をクリックします。

⑥ 右ペインの操作メニューにある[Start] をクリックします。

⑦ [Status] 欄が「Running」になったことを確認します。

9. 導入の流れ

▶ 暗号化の対象を決定します

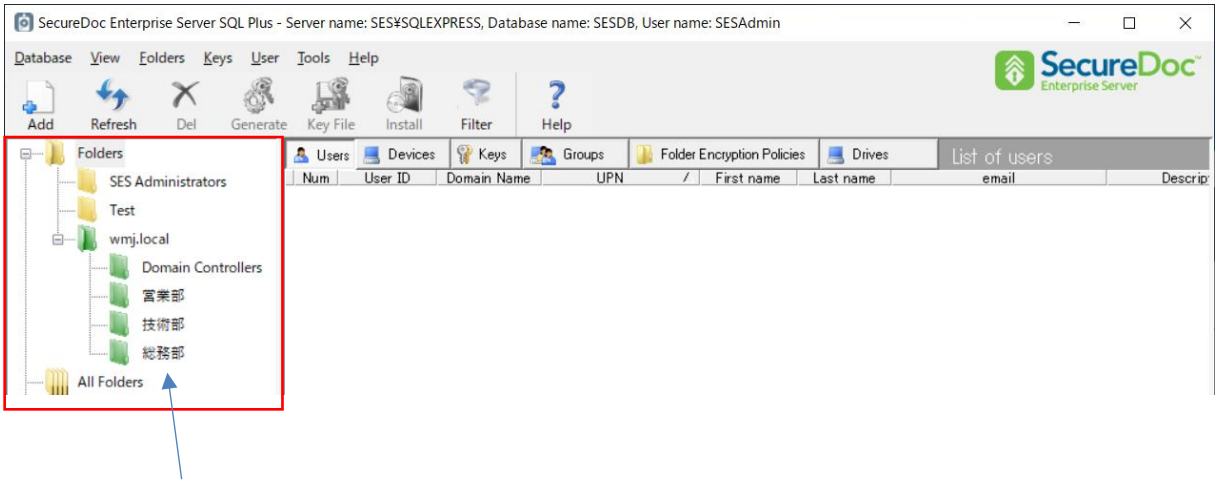
デバイスのディスクのみを暗号化し SES で管理する場合でも、通常の HDD/SSD の他、TCG Opal 自己暗号化ドライブや、既に BitLocker で暗号化済デバイスのセキュリティ強化等、企業によってデバイスの環境は異なります。
メディア暗号やファイル暗号の機能、設定方法の詳細については、「SecureDoc Enterprise Server Version 9.2 リファレンス マニュアル」を、ご参照ください。

▶ 展開方法を決定します

プロビジョニンルールを使った展開方法で、どのパターンを使用するかを決定します。
プロビジョニンルールを使わない展開方法については、「SecureDoc Enterprise Server Version 9.2 リファレンス マニュアル」を、ご参照ください。

▶ SES の各種設定

グローバルオプション（パスワードルール、ユーザー権限の設定、ライセンスの登録、コマンド有効期限）の設定
フォルダの作成、共有鍵の設定、管理者 ID を作成します。
ADSync を使って、Active Directory から OU をインポートすると、OU がフォルダとして登録されるので、フォルダを作成する必要はありません。

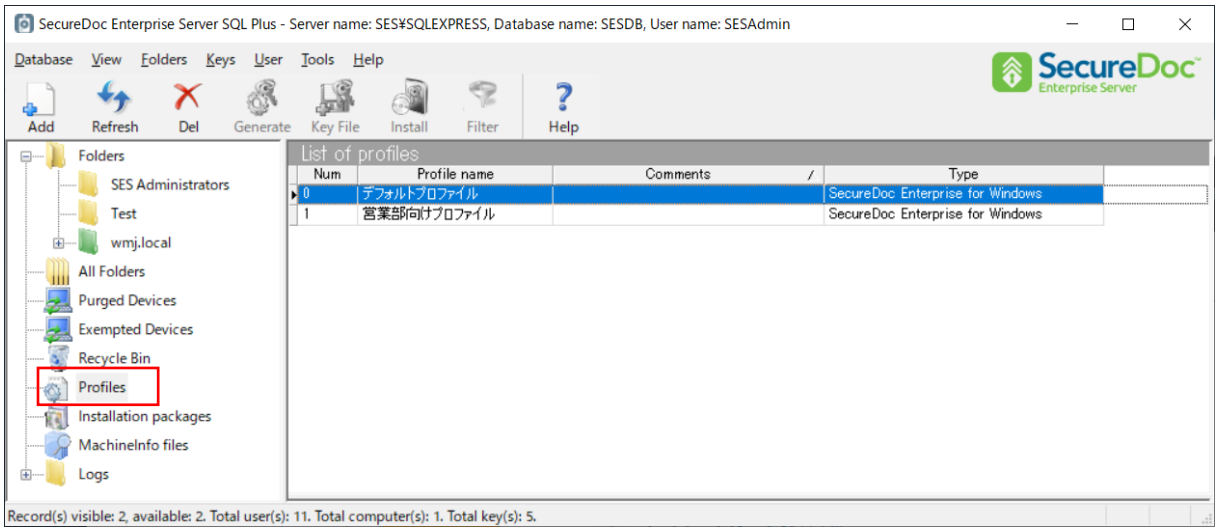


※ ADSync を使って OU をインポートすると、緑色のフォルダアイコンで表示されます。
SES 管理者が手動で作成したフォルダは黄色のフォルダアイコンになります。

※ フォルダ単位で、フォルダ内のデバイスに同じプロファイルを適用することや、メディア暗号用の共有鍵や管理者 ID を一斉に配備することができます。（削除も可）

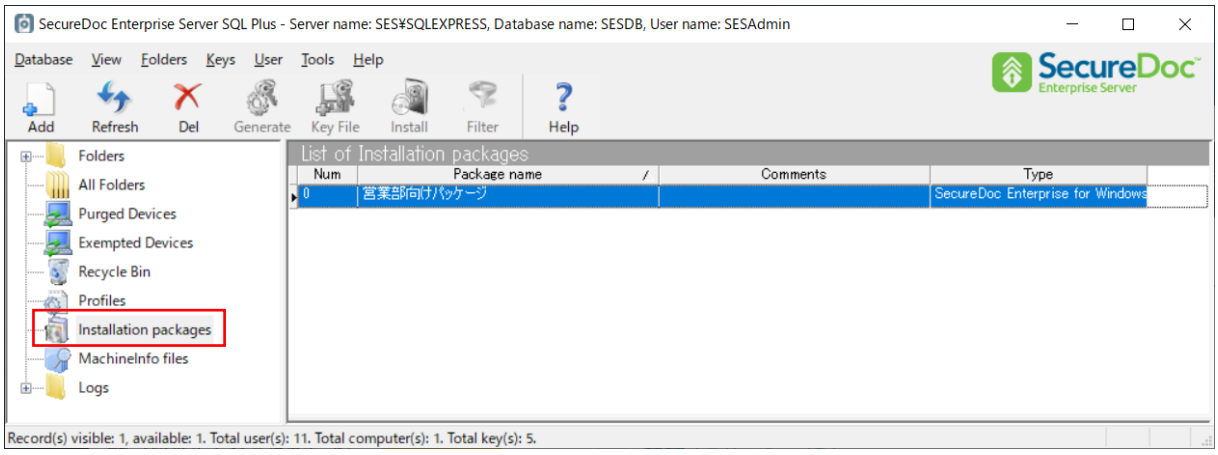
▶ プロファイルの作成

SecureDoc クライアントの動作に関する設定を決定します。ディスクの暗号化範囲、通信間隔、無通信猶予期間、シングルサインオン有無、パスワード失敗許容数等を設定します。プロファイルは複数作成できます。



▶ インストレーションパッケージの作成

「ユーザー登録先フォルダ」の指定や「ユーザー作成方法」、「プロファイル」の指定、「プロビジョニングルール」等の設定をします。



▶ SecureDoc Enterprise for Windows のインストール

インストレーションパッケージを使用して、クライアントに SecureDoc をインストールします。
希望通りの動作となっているか確認します。必要に応じて、グローバルオプション、SDConnex、プロファイル、インストレーションパッケージ等の設定を見直します。

10. プロビジョニングルールによる導入展開方法

『プロビジョニングルール』（導入展開方法）により、インストールから利用開始まで、企業での様々な導入形態に対応できます。プロビジョニングルールによる SecureDoc のクライアントインストールでは、インストールの実行からエンドユーザーが利用開始できる状態までをサイレントインストールで済ませることや、情報システム部門の担当者等デバイスの所有者以外が、利用者のパスワード設定だけを残してセットアップを完了し、ユーザーに SecureDoc クライアントを配備することも可能です。

10.1. ユーザーID の作成方法について

クライアントへの SecureDoc インストール時に、個々のユーザーID は自動で作成されるので、あらかじめ SecureDoc のユーザーID を作成する必要はありません。Windows ユーザーと同じ名前（Windows サインイン名）の ID をインストレーションプロセス中に自動で作成します。 SAM アカウントだけでなく、v8.6 以降は UPN にも対応しています。

SAM（SamAccountName）：**「ドメイン名¥ユーザー名」**
UPN (User Principal Name)：**「ユーザー名@Active Directory ドメイン名」**

注　Windows サインイン名から作成する SecureDoc の ID のパスワードは、Windows のパスワードと同期する必要があり、プリブート認証で使用するパスワードは Windows と同じパスワードを使用します。

※　Windows サインイン名以外にも、事前に SES で作成した ID やデバイス名から ID を作成することも可能です。

※　SES に事前に登録済のユーザーID のみを SecureDoc クライアントに配備することもできます。
詳しくは、「8.3 SDConnex サービスの開始」をご参照ください。

10.2. パスワード設定について

SecureDoc には、デバイスを利用する所有者としての「オーナー」という概念があり、ユーザーのパスワードが設定されるまで、デバイスにオーナーは登録されません。プロビジョニンルールを使った展開では、Windows サインインに使用した ID 及びパスワードを使用しオーナーの ID を作成するため、パスワードの入力すら不要です。管理者はユーザーのパスワード入力に関与する必要はありません。

10.3. パスワード同期について

パスワード同期によって、ユーザーが SecureDoc のパスワードを変更すると、Windows のパスワードも変更されます。パスワード同期によって、エンドユーザーは、ひとつのパスワードを憶えるだけでよく、パスワードルールの厳格化を実践するのに役立ちます。
同様に、Windows のパスワードを変更すると、SecureDoc のパスワードも変更されます。
注　この場合は、SecureDoc のパスワードルールは適用されず、Windows のパスワードルールに従います。

10.4. Credential Provider の利用について

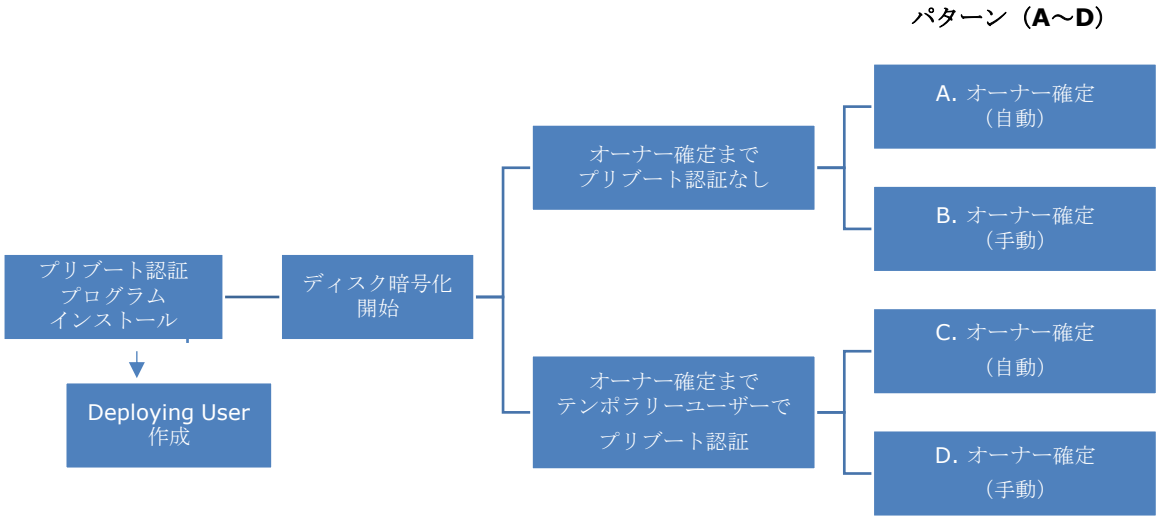
SecureDoc「Credential Provider」を設定すると、SecureDoc のパスワードルールによる Windows サインインとなり、シングルサインオン（SSO）の設定も可能です。SSO では、プリブート認証でログインに成功すると、Windows のサインインはパスされます。ユーザーの利便性を下げずに、パスワードルールの厳格化に役立ちます。

ワークグループ環境のデバイスについて：

パスワードルールが設定されていない Windows デバイスで、簡単なパスワードに変更されると、管理者が望まないようなパスワードで、プリブート認証および Windows にサインインできてしまう恐れがあります。
Windows にパスワードルールが設定されていない場合、SecureDoc の「Credential Provider」の利用を検討してください。

10.5. プロビジョニンルールのパターン

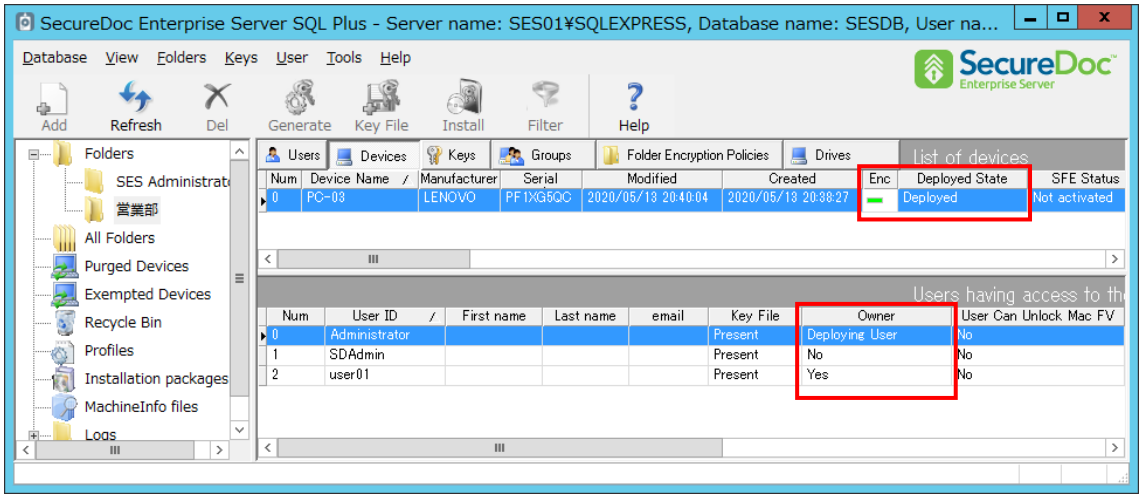
プロビジョニングルールを使用しての SecureDoc クライアントインストールは、次の 4 パターン（A～D）から選択できます。



SecureDoc クライアントをインストールすると、プリブート認証プログラムのインストールと共に「Deploying User」を作成し、暗号化を開始します。その Deploying User をそのままオーナーの ID とするのが、「パターン A」です。デバイス所有者自身がインストールする場合に適しています。また、BitLocker で暗号化済のデバイスに、エンドユーザー自身がインストールする場合にも適しています。

デバイス利用者以外の、例えば IT 部門等がインストールする場合は、エンドユーザーによる簡単な操作でオーナーを作成できる「パターン B」と「パターン D」が適しています。例えば、キッティング用のアカウントで Windows にサインインし、インストールを実行すると、キッティング用のアカウント名で、Deploying User が作成されます。それとは別に、エンドユーザーの Windows サインインアカウント名から ID を作成し、オーナーの ID とすることができます。

SES コンソールでは、全てのパターン（A～D）で、暗号化の状態やオーナーが確定し配備が完了しているかについて把握できます。次の図は、パターン B でイントールしたデバイスの状態を表しています。



パターン A （オーナー確定まで、プリブート認証なし、自動でオーナー確定）

「暗号化」、「オーナー確定」まで、全て自動でおこなうサイレントインストールが可能です。
インストールを実行すると、プリブート認証プログラムのインストールと共に、Windows へサインインしたアカウント名と同名の「Deploying User」を作成し、暗号化を開始します。Deploying User は、SecureDoc クライアントを配備するための ”仮のユーザー” です。暗号化の完了に関係無くデバイスを再起動すると、パターン A では Deploying user の ID を自動的にオーナーの ID に変更します。

注　Deploying User は、Windows にサインインしているアカウント名及びパスワードから作成し、それをオーナーの ID/パスワードとして設定しますので、デバイス所有者のユーザー自身がインストールする場合に適しています。

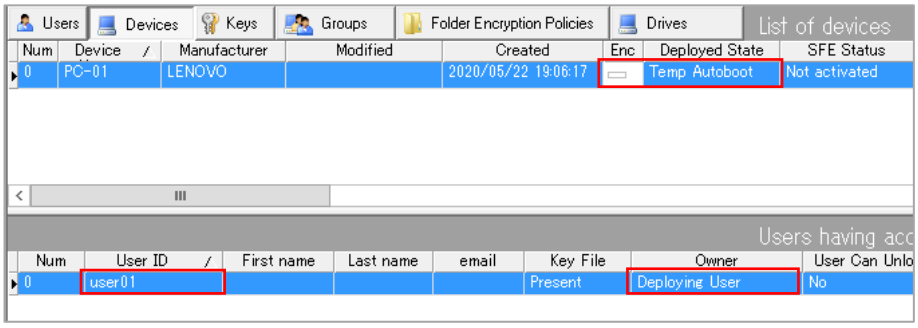
注　Windows サインイン名から作成したオーナーID のパスワードは、Windows のパスワードと同期する必要があり、プリブート認証で使用するパスワードは Windows と同じパスワードを使用します。

※　BitLocker で暗号化済のデバイスに、エンドユーザー自身がインストールする場合等に適しています。

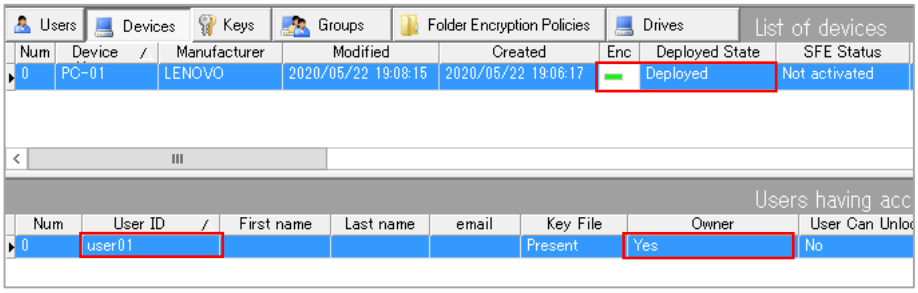
（例）

① エンドユーザーが、自身の Windows アカウント（例：user01）でサインインし、インストレーションパッケージを実行する。

② Deploying User の ID として、「user01」が作成される。



③ 再起動時、「user01」で Windows サインイン。Deploying User の「user01」は、オーナー（Owner）としての ID に自動で変更され、配備が完了したステータスに変わる（Deployed）。



④ オーナーが確定したことで、電源投入時に SecureDoc のプリブート認証が起動するようになる。
プリブートでの ID は「user01」、パスワードは Windows アカウント「user01」と同じパスワードを使用する。

⑤ プロファイルで、シングルサインオン(SSO)の設定が含まれている場合は、自動で設定される。

パターン B（オーナー確定まで、プリブート認証なし、オーナー確定は手動）

IT 部門の担当者が、キッティング用の Windows アカウントを使ってインストールする場合に適した展開方法です。
インストールを実行すると「暗号化」までを自動でおこない、エンドユーザーによる簡単な操作で、プリブート認証に必要な ID が作成されます。

インストール時に、Windows へサインインしたアカウントと同名の Deploying User を作成し、暗号化を開始します。Deploying User は、SecureDoc クライアントを配備するための ”仮のユーザー” です。暗号化の完了に関係無くデバイスを再起動すると、パターン A と異なり「SecureDoc プライマリアカウントの設定」ダイアログ画面が表示されます。ここで、<OK> をクリックすると、オーナーが確定しプリブート認証に必要な ID が作成されます。

「SecureDoc プライマリアカウントの設定」ダイアログ画面で、<後で>をクリックすれば、オーナーは確定しません。パターン B では、オーナーが確定するまで、プリブート認証は必要とされません。
エンドユーザーにデバイスを配備後、ユーザーが自身の Windows アカウントでサインインし、「SecureDoc プライマリアカウントの設定」ダイアログ画面で<OK>をクリックすると、Windows サインインアカウントと同名の SecureDoc ID が作成され、それがオーナーとしての ID となりパスワードも自動で設定されます。

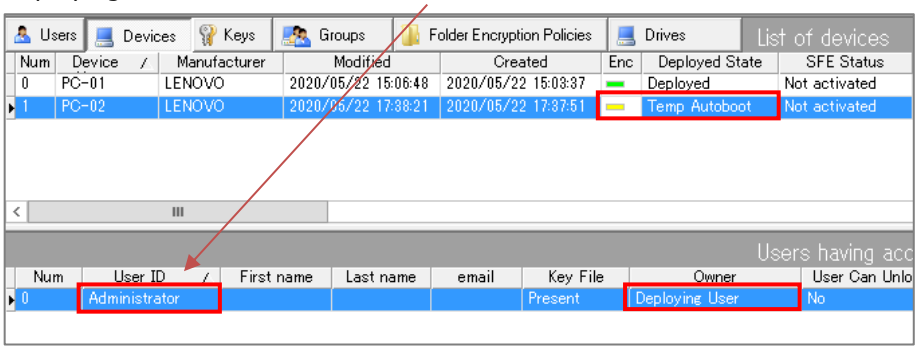
注　Windows サインイン名から作成したオーナーのパスワードは、Windows のパスワードと同期する必要があり、プリブート認証で使用するオーナーパスワードは Windows と同じパスワードを使用します。

※　<OK>をクリックするまで、「SecureDoc プライマリアカウントの設定」ダイアログ画面は Windows 起動後、常に表示されます。

（例）

① IT 部門が、Administrator アカウントで Windows サインイン後、インストレーションパッケージを実行する。

② Deploying User の ID として、「Administrator」 が作成される。



③ IT 部門では、「SecureDoc プライマリアカウントの設定」ダイアログで、常に<後で>をクリックする。

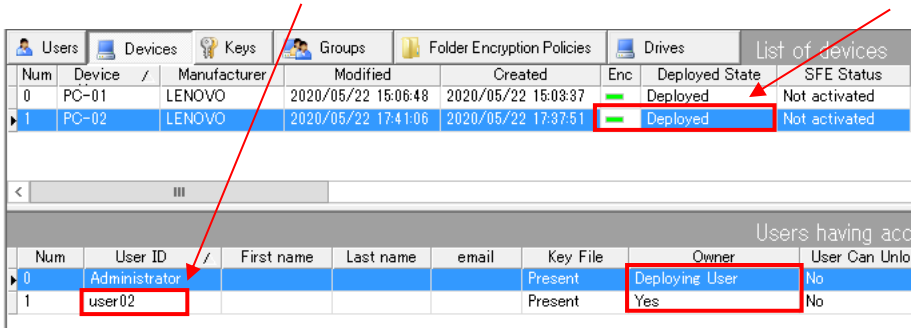
④ オーナーが確定するまで、OS 起動前のプリブート認証は必要とされず、表示されません（Temp Autoboot）。

⑤ 暗号化完了後、エンドユーザーにデバイスを提供する。

⑥ エンドユーザーが自身の Windows アカウント（例:user02）でサインインする。

⑦ 「SecureDoc プライマリアカウントの設定」ダイアログ画面が表示されるので、<OK>をクリックする。

⑧ オーナーとしての ID が自動で作成され、配備が完了したステータスに変わる（Deployed）。



⑨ オーナーが確定したことで、電源投入時に SecureDoc のプリブート認証が起動するようになる。
プリブートでの ID は「user02」、パスワードは Windows アカウント「user02」と同じパスワードを使用する。

⑩ プロファイルで、シングルサインオンの設定がされている場合は、SSO の設定も自動でおこなわれる。
プリブート認証で、Deploying User の ID「Administrator」は利用できません。

パターン C（オーナー確定まで、一時ユーザーでプリブート認証、自動でオーナー確定）

パターン A と異なるのは、オーナー確定まで、プリブート認証はオートブート（自動ログイン）ではなく、一時的に使用できるテンポラリーユーザーの ID とパスワードを使います。オーナー確定後、テンポラリーユーザーの ID は、クライアントデバイスから削除されます。

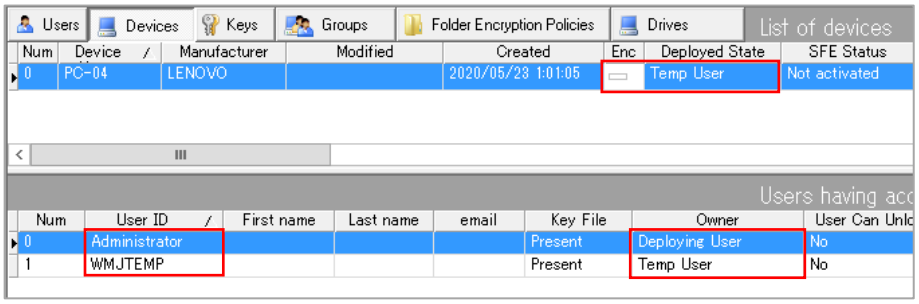
プリブート認証プログラムのインストール後の再起動で（暗号化の完了に関係無く）、Deploying user の ID を自動的にオーナーの ID に変更するので、このパターンは、キッティング等でデバイス所有者以外がインストールする場合には適しません。

パターン D（オーナー確定まで、一時ユーザーでプリブート認証、オーナー確定は手動）

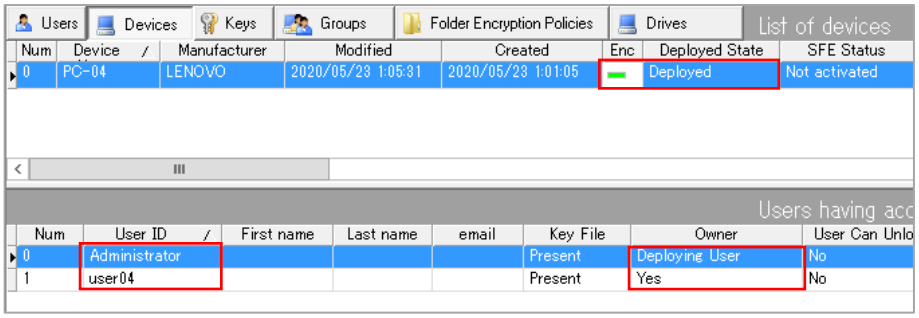
パターン B と異なるのは、オーナー確定まで、プリブート認証はオートブート（自動ログイン）ではなく、一時的に使用できるテンポラリーユーザーの ID とパスワードを使います。オーナー確定後、テンポラリーユーザーの ID は、クライアントデバイスから削除されます。「パターン B」よりもセキュアな展開方法です。

（例） Windows サインアカウント「Administrator」で、インストール

オーナー確定前、プリブート認証では、一時ユーザーの ID「例；WMJTEMP」でログイン



オーナー確定後、一時ユーザーの ID「WMJTEMP」は自動で削除される。



プロビジョニングルールを利用しない展開方法

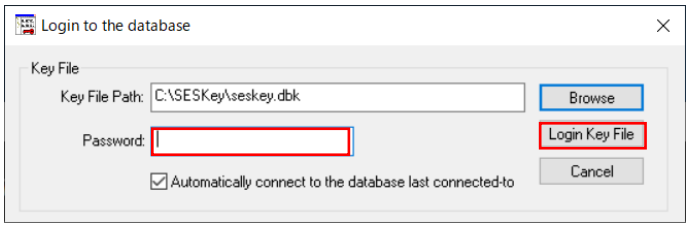
プロビジョニングルールを利用しない導入展開方法については、「SecureDoc Enterprise Server Version 9.2 リファレンス マニュアル」をご参照ください。

11. SES 管理コンソールについて

11.1. SES の起動

① [スタート] > [SecureDoc Enterprise Server] > [SecureDoc Enterprise Server]を実行します。

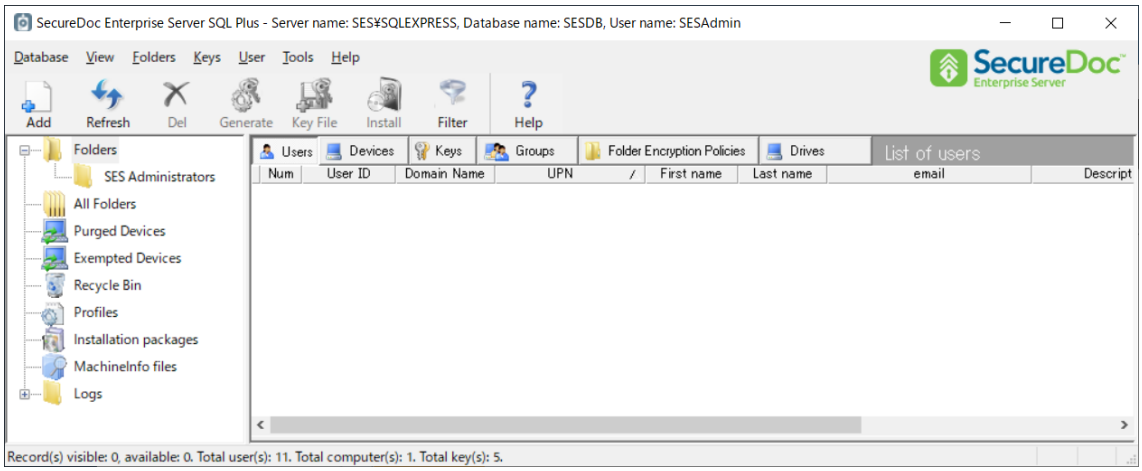
② ログイン画面が表示されますので、SES のインストール時に設定した管理者用のキーファイルのパスワードを[Password]欄に入力し、<Login Key File>ボタンをクリックします。



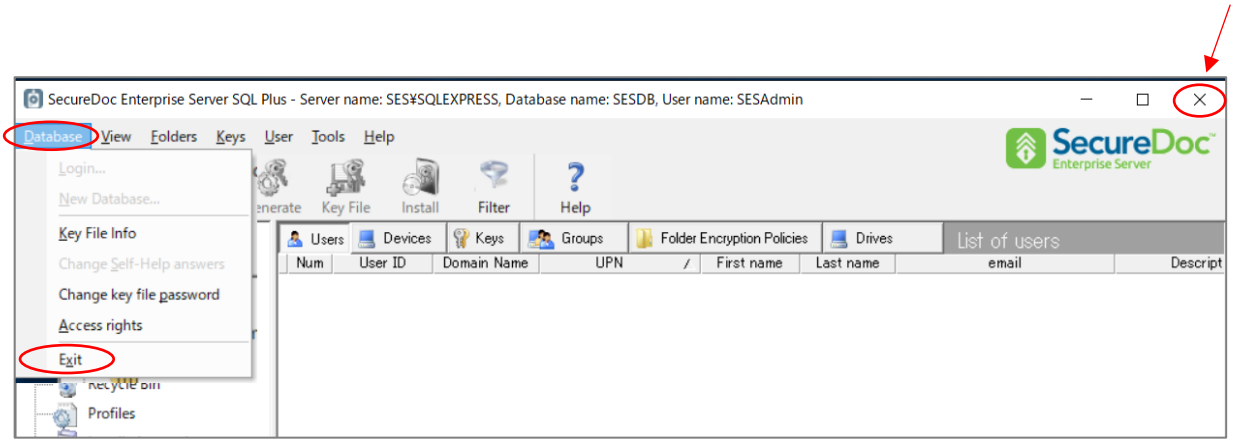
[Automatically connect to the database last connected-to]のチェックは、そのままにします。
複数の SES DB があり接続先を変更する場合、あるいは新規に DB を作成する場合は、チェックを外してログインします。

※ 旧バージョンからアップグレードした場合、DB のアップグレードについて確認のポップアップメッセージが表示されます。

③ SES の管理コンソール画面が表示されます。



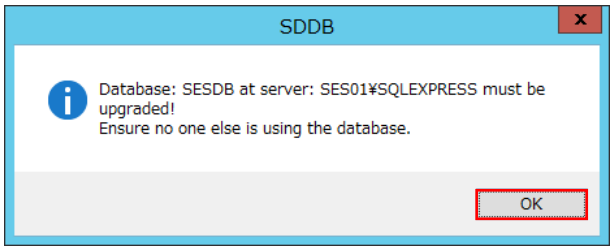
④ SES を終了する場合、[SES]ウィンドウの右上の<×>ボタンをクリックするか、[Database]-[Exit]メニューをクリックします。



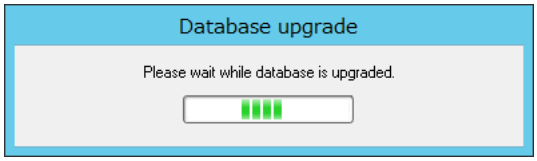
11.2. 旧バージョンからアップグレードした場合

① 旧バージョンからのアップグレードした場合、パスワード入力後、次の画面が表示されます。
<OK>をクリックして継続します。

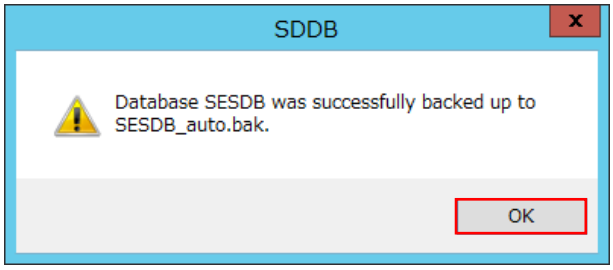
※ 表示されるデータベース名はお客様の環境により、異なります。



② DB のバックアップについての確認メッセージが表示されます。<はい>をクリックして、継続します。

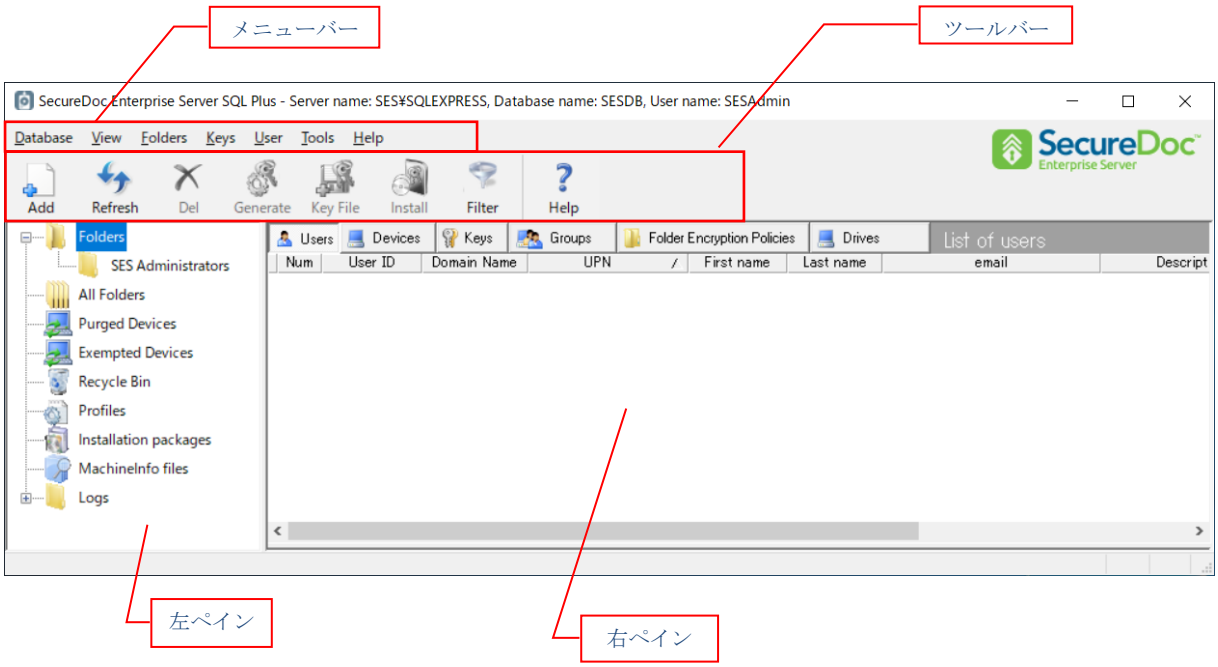


③ バックアップが成功すると、次の画面が表示されます。<OK>をクリックして継続します。
アップグレードしたバージョンにあわせて、データベースをアップグレードします。
アップグレードが完了後、<OK>をクイックすると、SES コンソールが起動します。



11.3. SES 管理コンソールの操作画面

左ペインには、ユーザーID やデバイス等の登録先である「Folders（フォルダ）」や「Profiles（プロファイル）」、「Installation packages（インストレーションパッケージ）」等のアイコンが表示されます。



アイコン名	説　明
Folders	Folders 配下には、SecureDoc クライアントのユーザー、デバイス、鍵、ステータス等の情報が格納されます。右ペインには、[Users]タブ、[Devices]タブ、[Keys]タブ等が表示されます。Folders 配下にサブフォルダを作成することができ、フォルダ単位で共有する暗号鍵やユーザーID を割り当てることもできます。 Microsoft Active Directory と連携した場合、Folders 配下に OU が表示されます。
All Folders	Folders 配下にある全てのフォルダに格納されているユーザー、デバイス、鍵、ステータス等の情報がまとめて表示されます。SecureDoc クライアント全体の登録状況を確認したい時に使用します。
Purged Devices	一定期間、SecureDoc クライアントが SES と通信しなかったデバイスを、不要なデバイスとして Purged Devices フォルダに移動できます。
Exempted Devices	SDConnex を使用してデバイスをプリブートネットワーク認証しているクライアントデバイスで、通信サイクルで指定された回数、SDConnex と通信しなかった場合、デバイスを Exempted Devices フォルダに移動させることが可能です。 このオプションの目的は、非通信デバイスをオートブートを許可しないグループに移動することにより、無人の常時接続のエンドポイントデバイス（IOT デバイス、自動預け払い機/自動販売機、キオスクデバイス等）のセキュリティを強化することです。 SDConnex と通信できない場合、デバイスが攻撃を受けているか、または危険にさらされている可能性があります（非通信期間中）。Exempted Devices フォルダに移動されたデバイスにはオートブートキーファイルが送信されないため、オートブートは実行されません。
Recycle Bin	ユーザー、デバイス、鍵を Folders から削除すると、Recycle Bin に移動されます。Recycle Bin 内のデータは、Folders に復元することができます。Recycle Bin から削除したデータは復元させることはできません。

アイコン名	説　明
Profiles	SecureDoc クライアントに適用したい各種設定をこの Profiles 配下に作成します。SecureDoc クライアントと SES が通信することで、各種設定がクライアント側に適用されます。[Profiles]アイコンをクリックすると、SES のデータベース上に存在するプロファイルの一覧が表示されます。
Installation packages	クライアントにインストールするためのインストレーションパッケージを作成します。
MachineInfo files	SecureDoc のクライアントへのインストールは、多くの設定は自動でおこなわれ、クライアントで作成されるユーザーID や鍵の情報は SDConnex を経由してデータベースに登録されます。SDConnex と通信できない環境でインストールする場合、それらの情報はクライアント PC に MachineInfo File として作成されます。クライアントで作成された MachineInfo File を SES に手動でインポートすることで、クライアント利用者のパスワードリカバリー等ができるようなります。
Logs	Audit Log、SFE Log、RME Log の 3 種類のログが格納されます。不具合等がある場合、必要に応じてログを参照します。

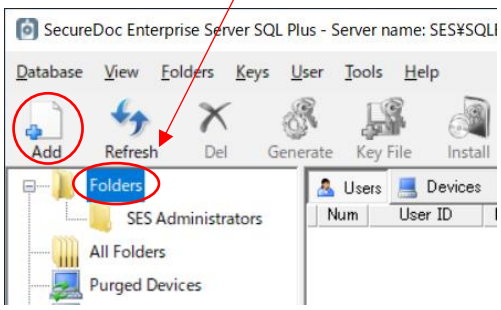
11.4. SES の操作方法

例として、フォルダを作成する場合の操作方法について、説明します。

ツールバーによる操作と、右クリックで表示されるメニューからの操作が可能です。

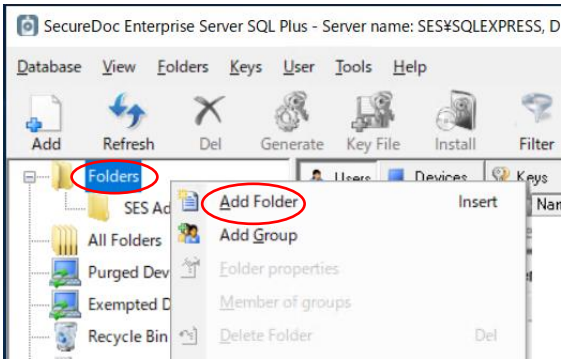
操作方法①

左ペインの「Folders」を選び、ツールバーの[Add]をクリックします。



操作方法②

左ペインの「Folders」を右クリックし、表示されたメニューから[Add Folder]をクリックします。



12. SES 各種設定

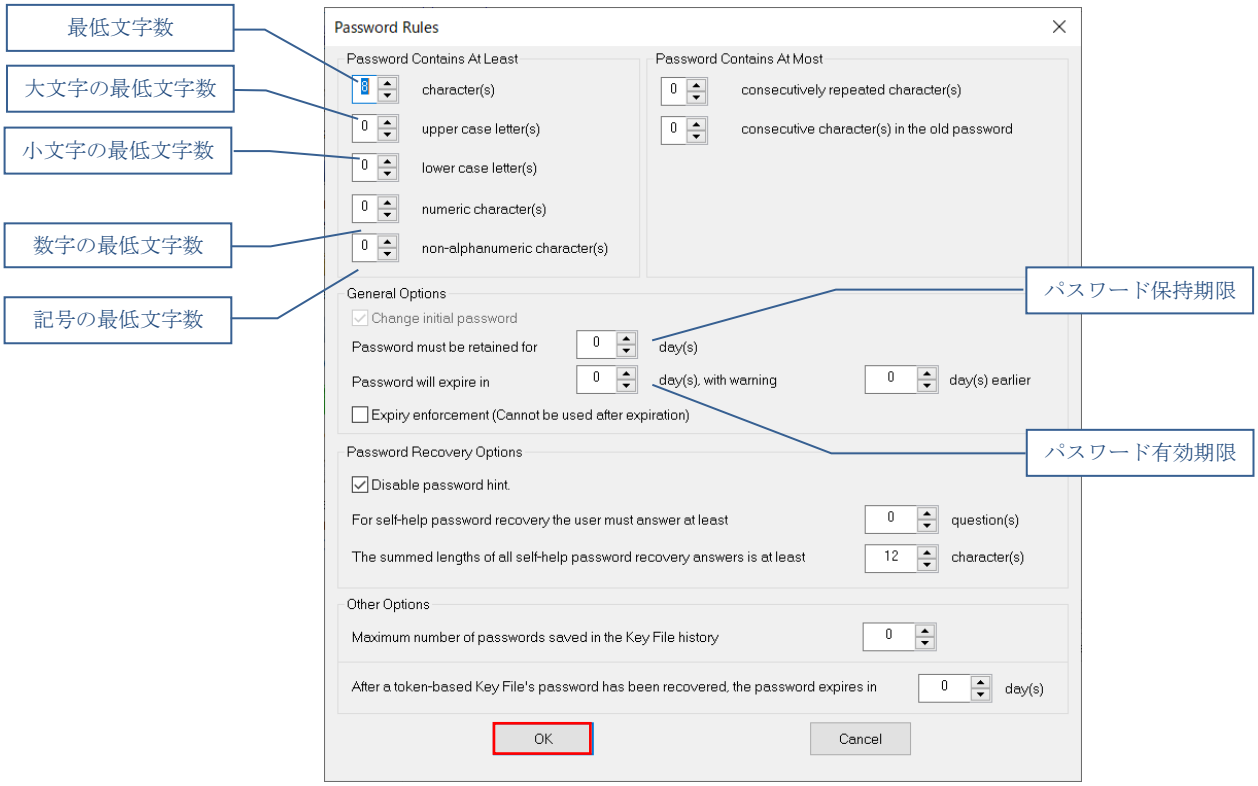
メニューバーの、[Tools] > [Options]で設定する項目を「グローバルオプション」と呼びます。
これには、SES 全体で有効となる各種設定項目があります。特に、パスワードルールの設定とクライアントインストールに必要なライセンスのインポートは必ず実施してください。

12.1. 【グローバルオプション】パスワードルールの設定

グローバルオプションには、全体で有効となるパスワードルールの設定があります。パスワードに関する内容として、「10.3.パスワード同期について」も参照してください。
ルールの設定は、インストレーションパッケージを作成する前におこなってください。

① [Tools]から[Options]をクリックします。
[Options]ウィンドウが表示されますので、下部にある<Password rules>ボタンをクリックします。

② 次の画面が表示されます。必要に応じて、パスワードルールを変更し、<OK>ボタンをクリックし保存します。
[Options]ウィンドウの下部にある<OK>ボタンをクリックして設定を保存します。



パスワードルール

項　目	説　明
Password Contains at least	パスワードに使用する最小文字数と文字の種類を指定します。
X　character(s)	パスワードの最低文字数を指定します。 デフォルトで「8」が設定されています。
X　upper case letter(s)	パスワードに含める大文字の最低文字数を指定します。
X　lower case letter(s)	パスワードに含める小文字の最低文字数を指定します。
X　numeric character(s)	パスワードに含める数字の最低文字数を指定します。
X non-alphanumeric character(s)	パスワードに含める記号の最低文字数を指定します。
Password Contains at most	パスワード内の最大文字数に関するルールを指定します。
X　consecutively repeated character(s)	パスワードに含めることができる同一文字の連続の最大数を指定します。0 を設定した場合、文字の連続使用を何回でも許可します。たとえば、「passssword」 も使用できます。1 を設定した場合、文字の連続使用を一切許可しないことを意味します。たとえば、「password」は使用できません。2 を設定した場合、文字の連続使用を 2 回まで許可します。
X consecutive character(s) in the old password	古いパスワードと新しいパスワードの間で共通して使用できる連続文字の最大数を指定します。たとえば、連続文字の最大数を 2 に指定し、古いパスワードが「PASSWORD」だった場合、新しいパスワードとして「WORLDMAP」は使用できません。これは、3 つの連続文字（「WOR」）が古いパスワードと新しいパスワードで共通しているためです。ただし、「WoRLDMAP」は「o」が小文字になっているため、使用できます。
General Options	パスワードの有効期限に関するオプションを設定します。
Change initial password	ユーザーが SecureDoc に最初にログオンしたときに初期パスワードの変更を求める場合は、チェックを入れます。デフォルトでは、チェックが入っています。プロビジョニングルールで設定したパスワードには適用されません。
Password must be retained for X day(s)	パスワードが保持される最低日数を指定します。
Password will expire in X day(s) with warning Y day(s) earlier	パスワードの有効期限を X に指定します。パスワードの有効期限を 30 日にしたい場合は、X を 30 にします。Y には、何日前から警告メッセージを表示させるかを指定します。
Expiry enforcement	チェックすると、パスワードの有効期限が切れると、キーファイルも有効期限切れになり、ユーザーはログインができなくなります。チェックしないと、パスワードの有効期限が切れても、ログインは可能です。ただし、新しいパスワードの入力を常に求められます。
Password Recovery Options	パスワードリカバリーに関するオプションを設定します。
Disable Password Hint	チェックをするとパスワードヒントが無効になります。 パスワードヒントの利用は推奨されません。
For self-help password recovery the user must answer at least X questions	セルフヘルプパスワードリカバリーを利用する場合に、ユーザーが答える質問数の最小値を指定します。 （注）セルフヘルプパスワードリカバリーは、日本語は使えません。

項　目	説　明
The summed length of all self-help password recovery answers is at least X character(s)	セルフヘルプパスワードリカバリーを利用する場合に、ユーザーが入力する質問の答えの合計文字数の最小値を指定します。
Other options	その他のオプションを設定します。
Maximum number of passwords saved in the key file history	パスワードの世代管理をおこないます。例えば 5 と設定すると、過去 5 世代の内に設定したパスワードを再利用することはできません。
After a token-based key file's password has been recovered the password expires in X day(s)	トークンを利用しているユーザーがパスワードリカバリーをおこなった場合、指定の日数だけパスワードだけでログインできるようになります。0 にすると、トークンがなければ、都度パスワードリカバリーをおこなう必要があります。

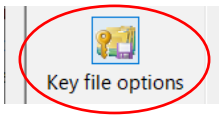
12.2. 【グローバルオプション】ユーザー権限の設定

初期設定では、パスワードの変更以外できない権限となっています。
インストールプロセスで作成されるユーザーに付与される権限です。SES 上で、個別にユーザーを作成する場合も、ここでの設定が初期設定になります。

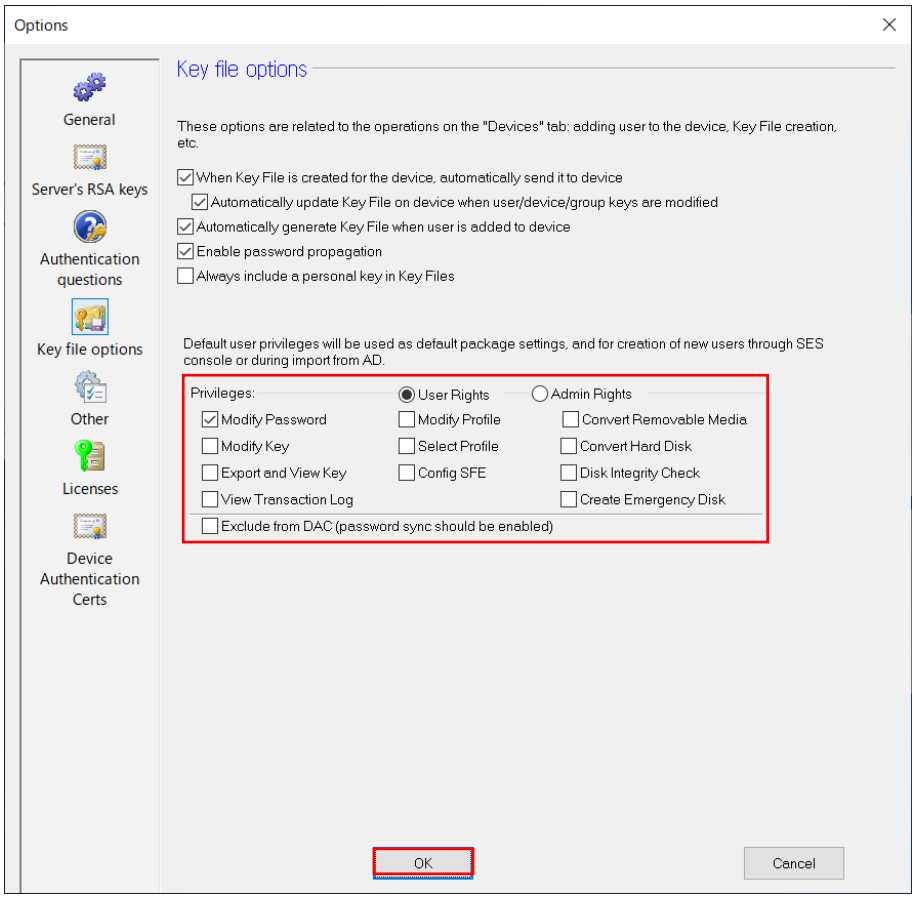
将来、メディア暗号やファイル暗号を使用する計画が予想される場合、それらに必要な権限を付与しておくことも検討します。権限を付与していても、プロファイルでリムーバブルメディアの暗号化やファイル暗号化の設定をしなければ、ユーザーがそれらを利用することはできません。

メディア暗号に必要な権限：　[Convert Removable Media]
ファイル暗号に必要な権限：　[Config SFE]

① [Tools]から[Options]をクリックします。
[Options]ウィンドウの、左ペインにある<Key file options>アイコンをクリックします。



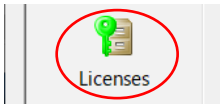
② 次の画面が表示されます。[Privileges]欄より付与したい権限のチェックボックスをオンにし、<OK>ボタンをクリックします。



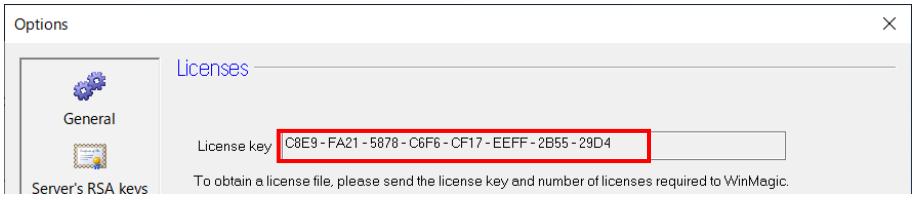
12.3. 【グローバルオプション】ライセンスのインポート

グローバルオプションには、ライセンスのインポートメニューがあります。11 台以上の SecureDoc クライアントを管理する場合は、下記の手順に従い、ライセンスファイルをインポートしてください。

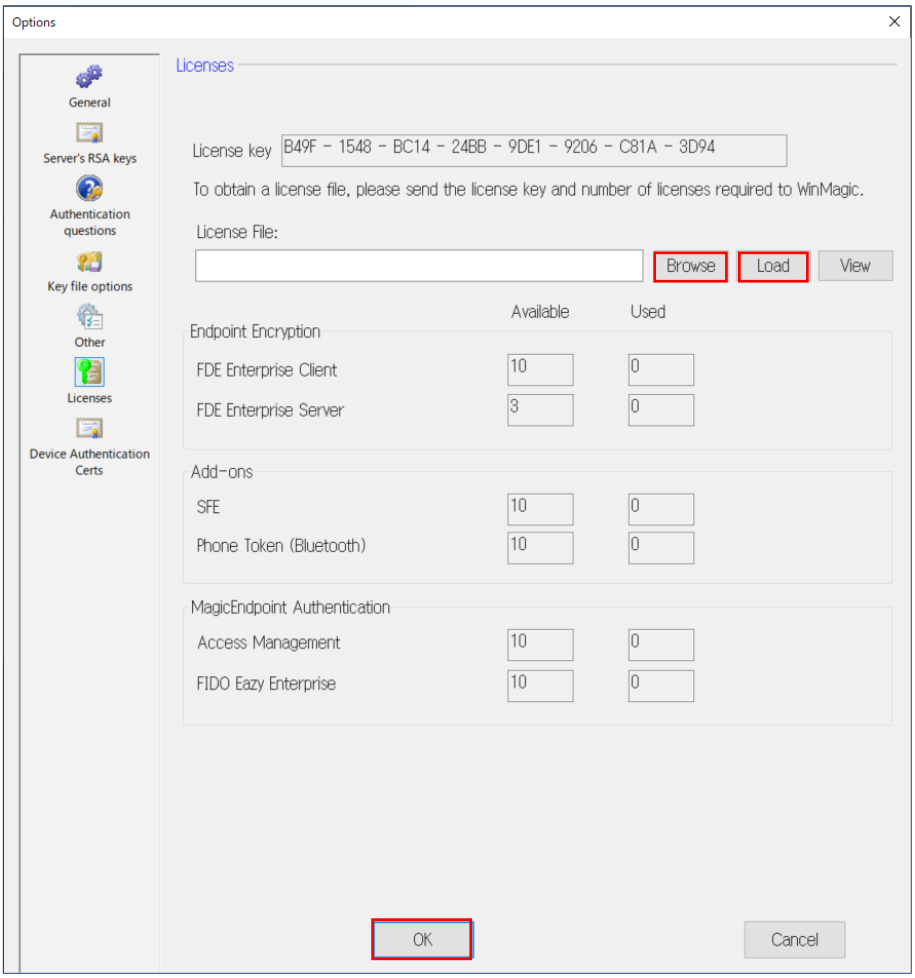
① [Tools]から[Options]をクリックします。
[Options]ウィンドウの、左ペインにある<Licenses>アイコンをクリックします。



② 次の画面が表示されます。[License Key]の値をライセンス購入元に伝え、ライセンスファイルを依頼します。



③ ライセンスファイル入手後、<Browse>ボタンをクリックして受領したライセンスファイルを選択します。
その後、<Load>ボタンをクリックしてライセンスをインポートします。



④　ライセンスファイルのインポートに成功し、[Available]の数量が増えていることを確認します。

⑤　下部にある<OK>ボタンをクリックして、ライセンス設定を保存します。

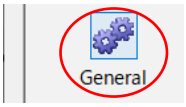
12.4.　【グローバルオプション】コマンド有効期限の設定

SES から発行したコマンドは初期設定で 30 日間の有効期限が設定されています。

一部の SecureDoc クライアントでも SES と通信しない期間が長くなることが想定される場合は、コマンドの有効期限を長く設定します。

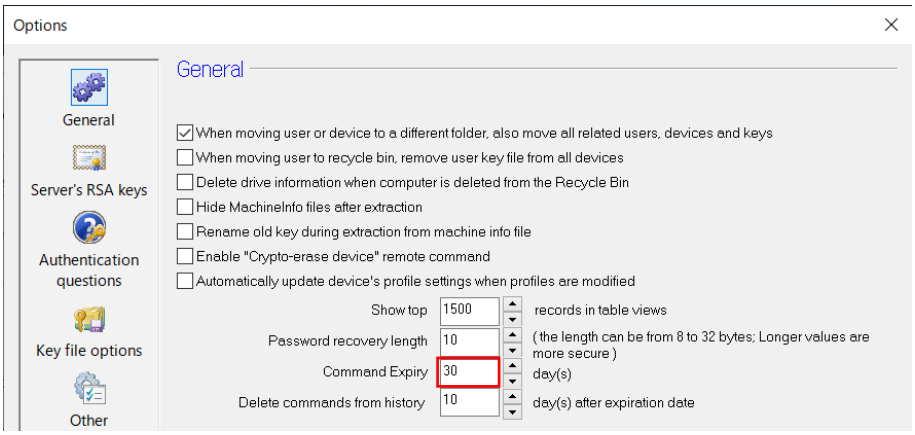
①　[Tools]から[Options]をクリックします。

[Options]ウィンドウの左ペインにある<General>アイコンをクリックします。



②　[Command Expiry]の有効期限を必要に応じ変更し、下部にある<OK>ボタンをクリックして設定を保存します。

以降、新しく発行するコマンドの有効期限が変更した値となります。



この後の設定は、クライアントへのインストールに必要な各種設定をおこないます。

12.5. フォルダの作成

フォルダは、「ユーザー」、「デバイス」、「暗号鍵」の登録先というだけでなく、フォルダ配下のデバイスへ共有暗号鍵（共有鍵）や共有の ID（例えば管理者権限の ID）を割り当てることができます。少なくとも 1 つのフォルダを作成するようにしてください。

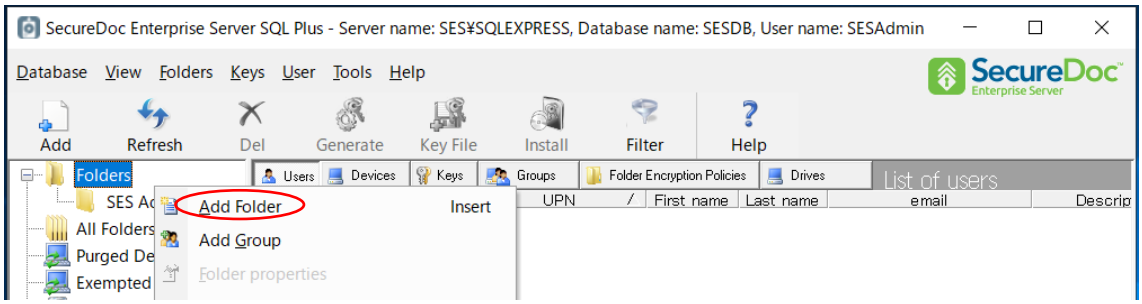
ADSync を使って OU をインポートした場合は、OU がフォルダとして機能しますので、SES でフォルダを作成する必要はありません。AD のユーザーには存在しないユーザーの為に、フォルダを作成し、OU から作成したフォルダと混在することも可能です。

フォルダに共有鍵を割り当てることで、そのフォルダに所属するユーザーID のキーファイルには、ディスク暗号鍵のほかに共有鍵が追加されます（キーファイルは再作成されます）。共有鍵が含まれたキーファイルをもつユーザーは、共有鍵で暗号化された暗号化メディアや共有フォルダへシームレスにアクセス可能となります。

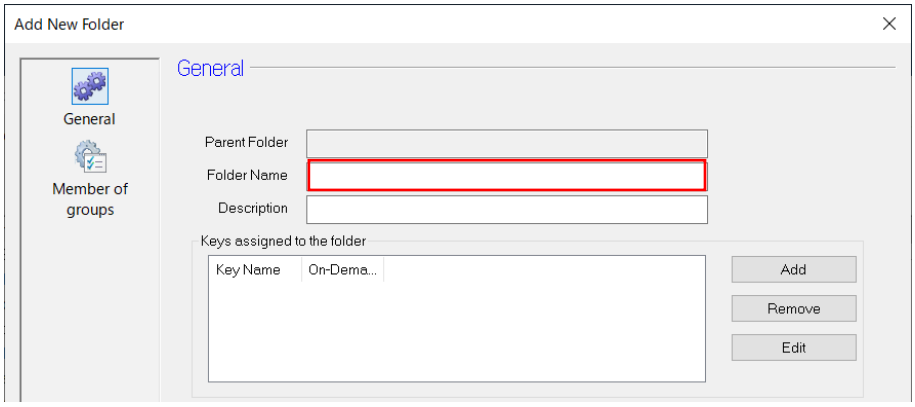
また、管理者 ID をフォルダに割り当てると、その配下にあるデバイスに、定期的な通信によって管理者 ID が追加されます。クライアントインストール前に、フォルダに管理者 ID が割り当てられていると、インストール時に管理者 ID がクライアントに追加され、フォルダに共有鍵が割り当てられていると、インストール時にユーザーのキーファイルに共有鍵が追加されます。

その他、フォルダ配下にあるデバイスに対して、フォルダ単位で同じプロファイルを割り当てることもできます。

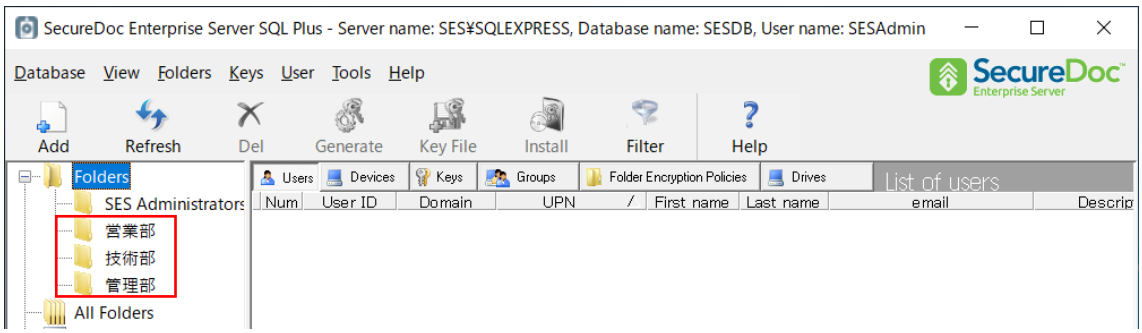
① 左ペインより、[Folders]アイコンを選択した状態で、ツールバーの[Add]をクリックするか、右クリックによるメニューから[Add Folder]をクリックします。



② 次の画面が表示されますので、[Folder Name]欄にフォルダ名を、必要に応じて[Description]欄に補足説明を入力し、<OK>ボタンをクリックし、フォルダを作成します。



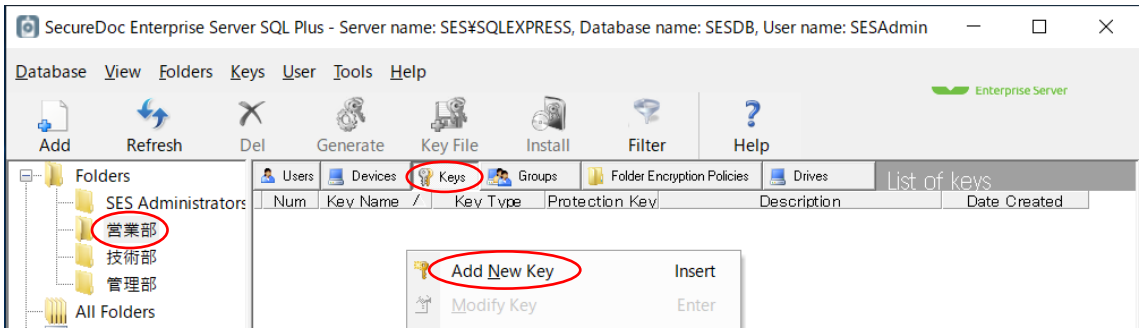
③ 他にもフォルダを作成したい場合、本手順を繰り返してフォルダを作成します。左ペインの[Folders]配下に作成したフォルダが表示されていることを確認します。



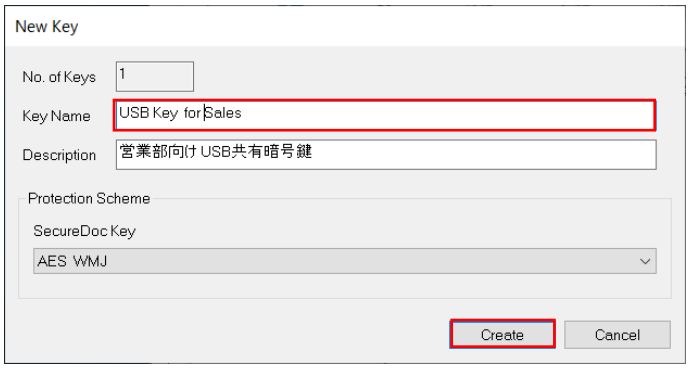
12.6. 共有鍵の作成（USB メモリやフォルダ暗号用）

ディスクを暗号化する場合、クライアント固有の暗号鍵を使用して暗号化します。それはインストール時に各々のクライアントで生成されます。一方、USB メモリや共有フォルダを暗号化する場合、共有の暗号鍵を使用して暗号化すると、共有鍵を持つ SecureDoc ユーザー間では、シームレスにデータの受け渡しが可能です。共有鍵を SES で作成して、ユーザーが登録されているフォルダや所属するグループに割り当てることができます。

① 左ペインより、共有鍵を作成したいフォルダ先をクリックします。次に右ペインより、[Keys]タブをクリックし、ツールバーの[Add]をクリックするか、右ペインの上で右クリックし、表示メニューから[Add New key]をクリックします。



② 次の画面が表示されますので、[Key Name]欄にキー名、必要に応じて[Description]欄に補足説明を入力し、<Create>ボタンをクリックします。



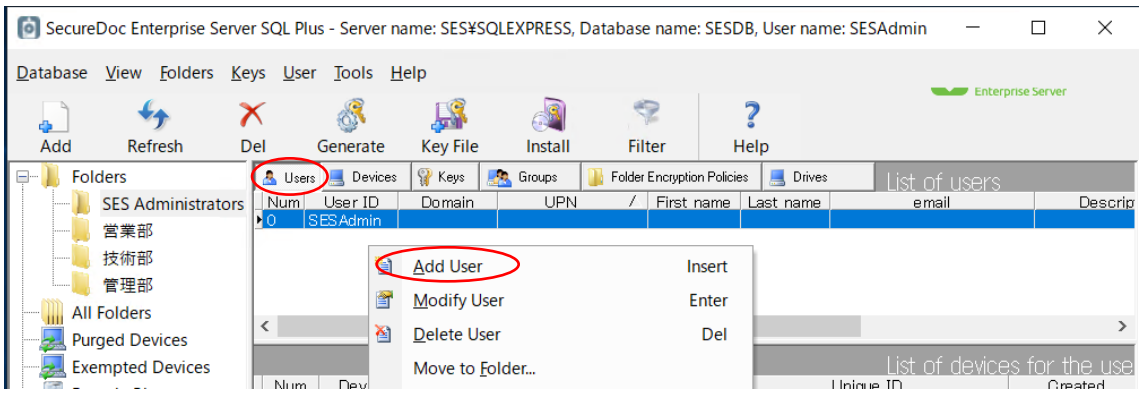
③ ”Key successfully created”というダイアログが表示されますので、<OK>ボタンをクリックします。

④ 他にもデータの受け渡しが必要なグループがある場合は、本手順を繰り返して共有鍵を作成します。
[Keys]タブ配下に、作成した共有鍵が表示されていることを確認します。

12.7. 管理者権限 ID の作成

通常、エンドユーザーの ID にはパスワード変更権限しか付与されていません。必要に応じて、SecureDoc クライアントに追加する管理者権限の ID を作成します。

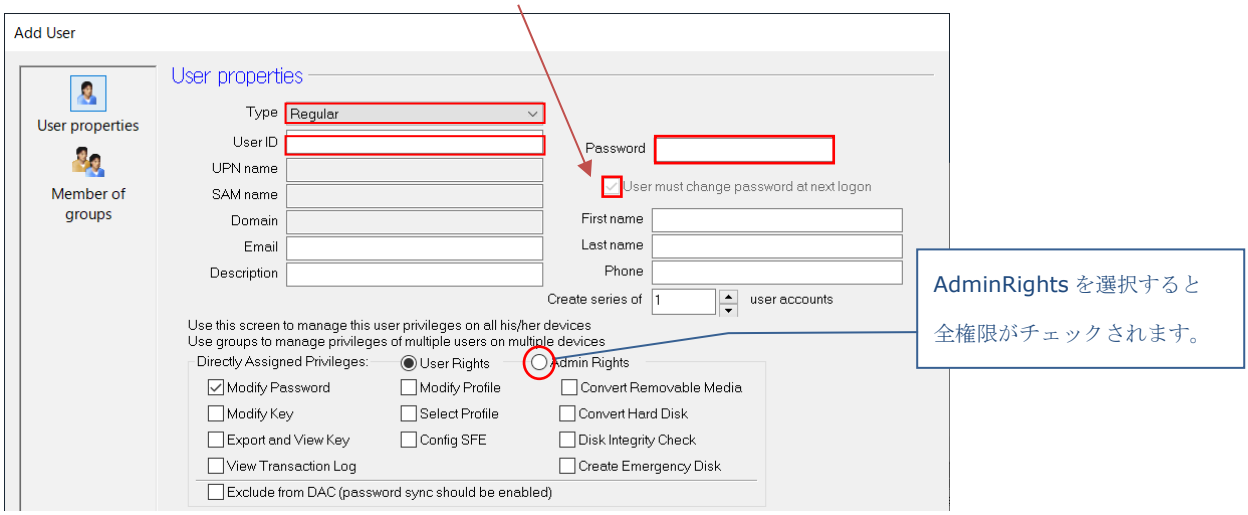
① 左ペインより、管理者権限ユーザーを作成したいフォルダを選択します。次に右ペインより、[Users]タブをクリックし、ツールバーの[Add]をクリックするか、右ペインの上で右クリックし、表示メニューから[Add User]をクリックします。



② [Type]のプルダウンメニューで、「Regular」を選択します。
[User ID]欄に管理者の名前を入力し、[Password]欄に強固なパスワードを入力します。

注 デフォルト設定では、[User must change password at next logon]が有効になっており、ここで設定したパスワードを使ってログイン後、Windows 上でパスワードの変更を求められます。

注　ここでは、エンドユーザーの為の ID ではなく、管理者 ID をクライアントに配備することを想定しているので[User must change password at next logon]のチェックを外します。



③　次に、[Directly Assigned Privileges]の項目で、[Admin Rights]ラジオボタンをクリックします。

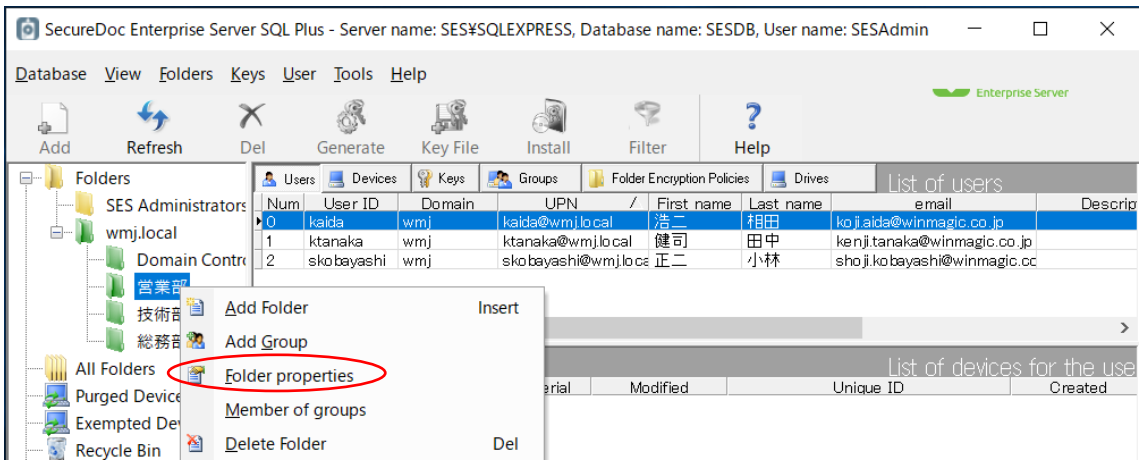
④　最後に、<Create>ボタンをクリックします。
指定したフォルダ配下に管理者権限ユーザーが作成されます。

12.8. フォルダの機能を使った管理者 ID の配備や共有鍵の追加

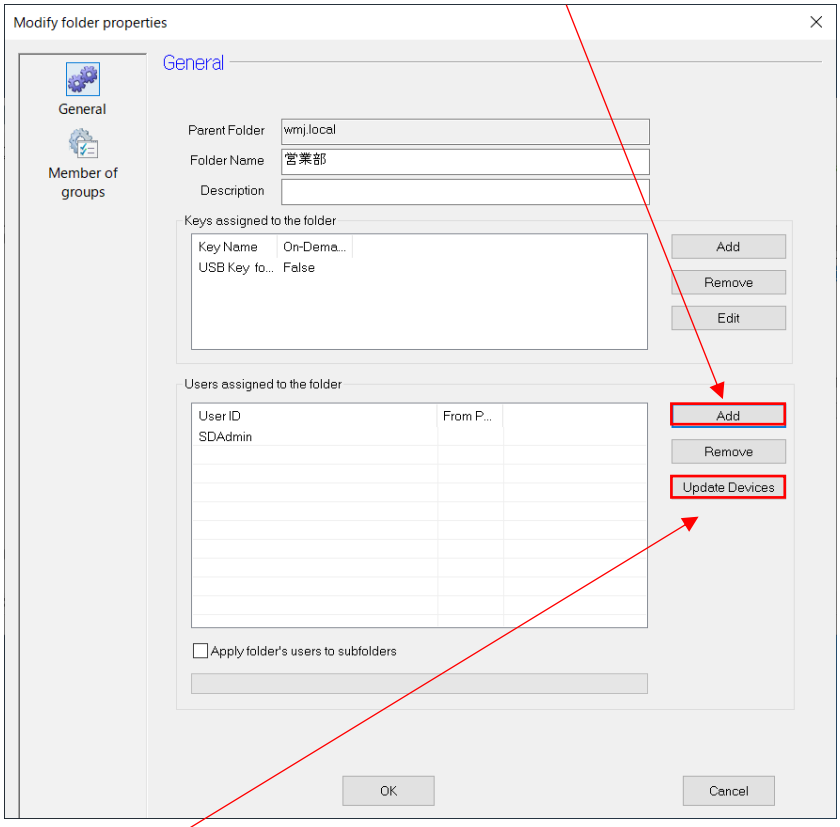
フォルダの機能で、管理者 ID をクライアントデバイスに登録することや、ユーザーのキーファイルに共有鍵を追加することができます。フォルダにそれらが設定されていると、クライアントのインストール時に自動で管理者 ID がクライアントデバイスに登録され、共有鍵がユーザーのキーファイルに追加されます。クライアントのインストール後に、それらを登録・追加したり、削除することもできます。

①　フォルダ機能を使って、管理者 ID をクライアントに配備します。
※　共有の一般ユーザー（管理者権限以外）もフォルダ機能で配備できます。

②　「Folders」下のフォルダを右クリックし、メニューから[Folders properties]をクリックします。



③ 「Users Assigned to the folder」の項目で、<Add>をクリックして、一覧にユーザーを追加します。



④ <Update Device>を実行すると、フォルダに登録されているデバイス全てに、そのユーザーを追加します。

※ クライアントのインストール前に、設定されていた場合、<Update Device>を実行せずともクライアントのインストール時に自動で追加されます。

⑤ クライアントは定期的な通信で、ユーザーを受け取り、二人目以降の ID として登録されます。

⑥ <Remove>をクリックし、一覧からユーザーを削除して、<Update Device>を実行すると、このフォルダに登録されているデバイス全てから、そのユーザーを削除します。クライアントは定期的な通信で、その命令を受け取りデバイスからユーザーは削除されます。

⑦ 同様に、「Keys Assigned to the folder」で、<Add>をクリックして、一覧に共有鍵を追加します。

※　クライアントのインストール前に、設定されていた場合、クライアントインストールのキーファイル作成時に自動で追加されます。

⑧　クライアントのインストール後に設定した場合、SES は、このフォルダに登録されているユーザー全てにそれぞれ共有鍵を追加したキーファイルを再作成し、クライアントは定期的な通信で、新しいキーファイルを受け取ります。

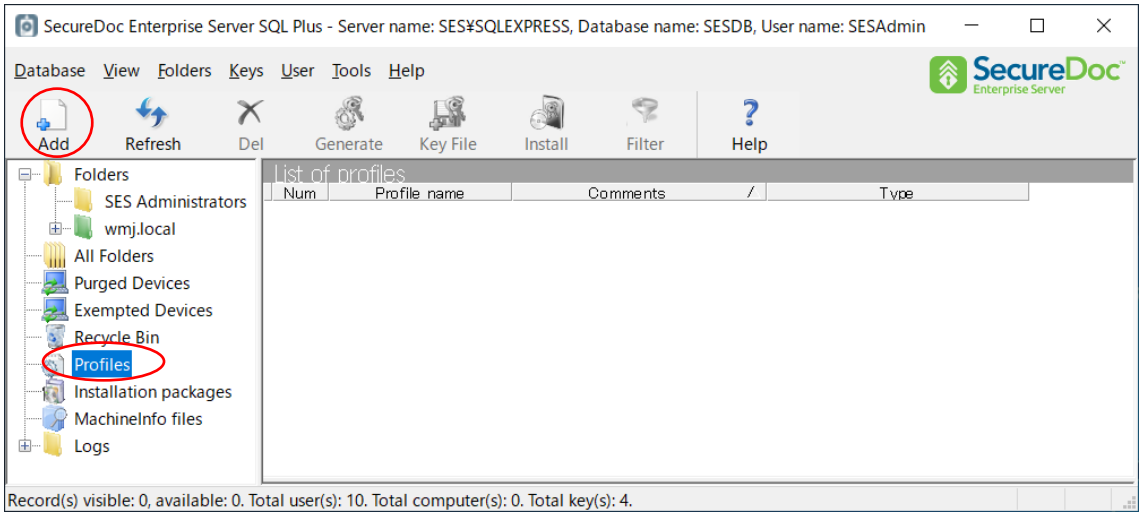
※　キーファイルの再作成によって、ユーザーのパスワードは変更されません。

⑨　<Remove>をクリックして共有鍵を一覧から削除すると、フォルダ配下のユーザーのキーファイルから共有鍵を削除したキーファイルをそれぞれ再作成し、クライアントは定期的な通信で、新しいキーファイルを受け取ります。

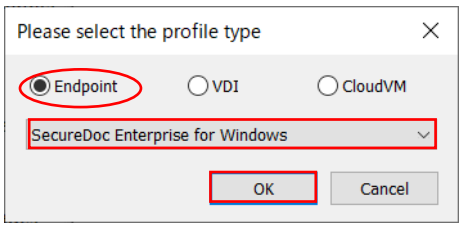
13. Windows 用プロファイルの作成

「SecureDoc Enterprise for Windows」ライセンスを使用する Windows クライアント用のプロファイルを作成します。

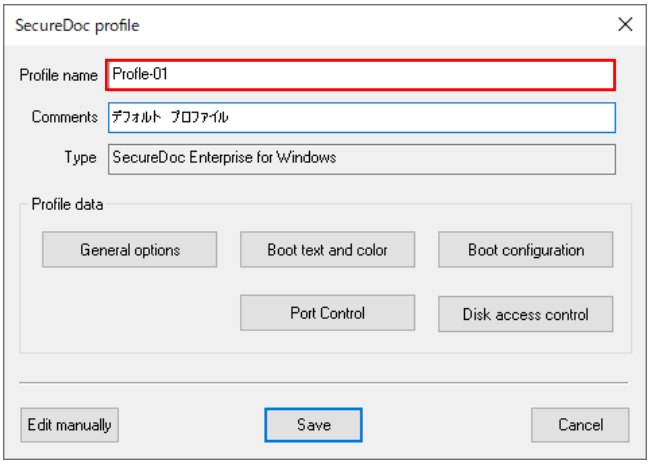
①　左ペインの[Profiles]アイコンを選択し、<Add>ボタンをクリックするか、右ペインの上で右クリックし、表示メニューから[Add profile]をクリックします。



②　[Please select the profile type]ウィンドウが表示されますので、[Endpoint]のプルダウンメニューより「SecureDoc Enterprise for Windows」を選択し、<OK>ボタンをクリックします。



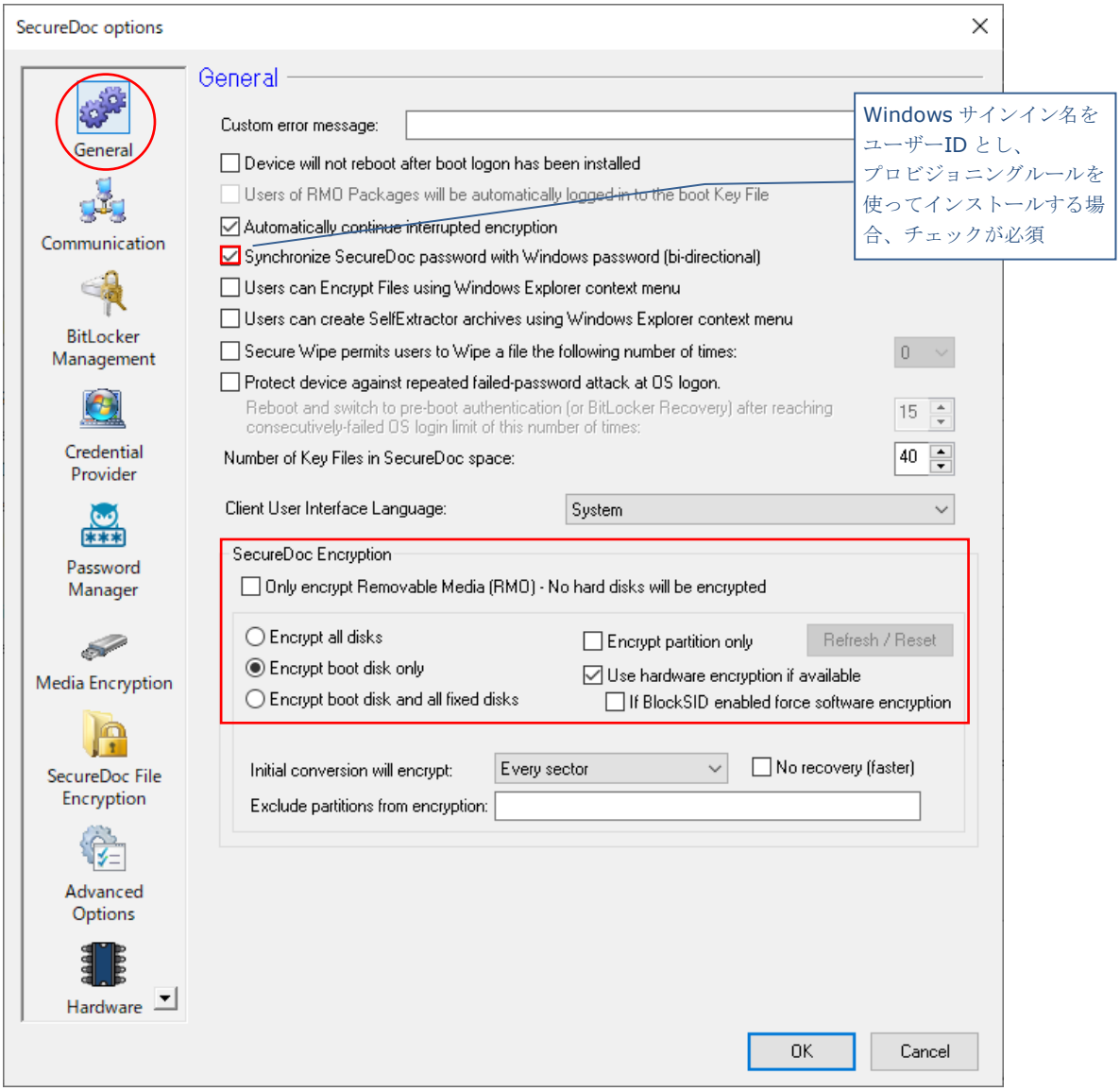
③　[Profile name]欄にプロファイル名を、必要に応じて[Comments]欄にコメントを入力します。



13.1. General options の設定

① プロファイル作成トップ画面から、<General options>ボタンをクリックします。

② 左ペインにある[General アイコンが選択されます。ここでは主にディスク暗号化の設定をおこないます。



注 Windows サインイン名をオーナーの ID とするプロビジョニングルールを使ってインストールする場合、[Synchronize SecureDoc password with Windows password(bi-directional)]のチェックが必要です。

[SecureDoc Encryption]の設定項目で、暗号化対象を選択します。

注 BitLocker で暗号化済のデバイスにインストールする場合や、BitLocker の暗号化機能を使用する場合、これらの設定は無視されます。この設定は、SecureDoc のエンジンで暗号化する場合に使用されます。

○ Encryption all disks … 全てのディスクを暗号化します。

◎ Encryption boot disk only … ブートディスクのみ暗号化します。（初期設定）

○ Encryption boot disk and all fixed disks …. 固定ディスク全てを暗号化します。

☐ Encryption partition only … パーティションを暗号化します。

☑ Use hardware encryption if available …

インストレーションパッケージが、ハードウェアレベルの暗号化機能を有する TCG Opal ドライブを検知した場合、ソフトウェアによる暗号化はおこなわず、ドライブを Opal モードに変更し、Opal モードに必要とされるプリブート認証プログラムをインストールします。暗号化に要する時間が不要のため、短時間で、インストールが完了します。チェックを外していた場合は、TCG Opal ドライブであっても Opal モードに変更せず、ソフトウェアで暗号化します。

注　事前に UEFI / BIOS 設定で、HDD パスワードもしくは Block SID の設定を無効にしておく必要があります。UEFI の制限で Block SID を解除できないデバイスの場合、TCG Opal ドライブであってもソフトウェアで暗号化する必要があり、このオプションのチェックを外してください。

注　TCG Opal ハードウェアの仕様で、インストール完了時、シャットダウンが必要です。

[Initial conversion will encrypt:]

○ Every sector … 全てのセクターを暗号化します。

◎ Data only(faster) …

インストール時、ディスクの使用済領域のみを暗号化します。SecureDoc のインストール完了後、データが書き込まれると、そのセクターは自動で暗号化されます。暗号化をユーザーが意識することはありません。

注　既にユーザーが使用しているデバイスにインストールする場合、このオプションは推奨されません。新しいデバイスを暗号する場合に使用してください。

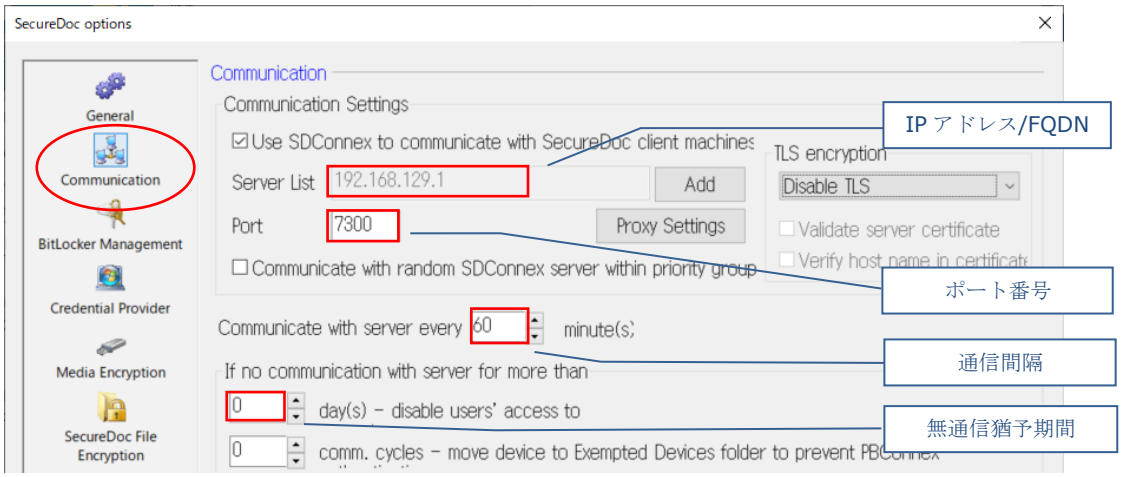
No recovery(faster) …

リカバリデータを作成せずに暗号化を実行することで、暗号化プロセスが高速化されます。このオプションは、新しいドライブをすばやく暗号化する必要がある場合に役立ちます。

注　既にユーザーが使用しているデバイスでは使用しないでください。

注　このオプションを選択する場合、暗号化中、電源を切らないでください。
このオプションを選択していない場合、暗号化中でもデバイスをシャットダウン可能です。電源を入れると暗号化を自動で再開します。

③　次に、左ペインにある[Communication]アイコンをクリックします。
SDConnex との接続に必要な IP アドレス、ポート番号、通信間隔、必要に応じて無通信猶予期間を設定します。



「Server List」で、SDConnex をインストールしたサーバーの IP アドレスがリストにあることを確認します。IP アドレスが異なる場合、<Add>をクリックして、該当の IP アドレスを追加します。ポート番号は、7300 がデ

フォルト設定です。

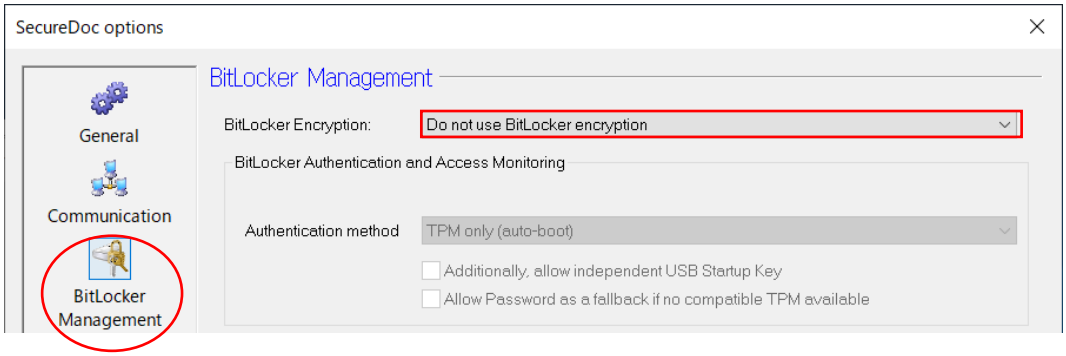
通信間隔は、SecureDoc クライアントが SDConnex と通信する間隔です。クライアントは起動時、もしくは初回疎通時に SDConnex と通信すると、その後はここで設定された間隔で SDConnex との通信を試みます。

無通信猶予期間の設定は、[If no communication with Server for more than]の項目で、[x days(s) – disable user's access to computer]を設定すると、設定日数内に SDConnex と通信が無かった場合、クライアントデバイスのキーファイルをロックします。ロックされると、エンドユーザーがプリブート認証で正しい認証情報を入力してもログインできなくなります。解除するには、SES の管理者に連絡し、チャレンジレスポンスによるリカバリー操作が必要です。

④ BitLocker で暗号化済のデバイスにインストールする場合や、BitLocker の暗号化機能を使う場合は、[BitLocker management]アイコンをクリックします。

注　SecureDoc の機能で暗号化する場合や、TCG Opal ディスクへのインストールでは、この設定は不要です。

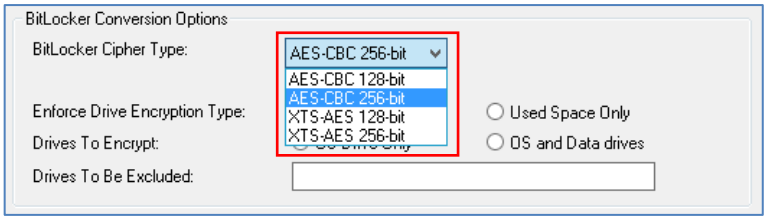
[BitLocker Encryption:] のプルダウンメニューで、プリブート認証方法を選択します。



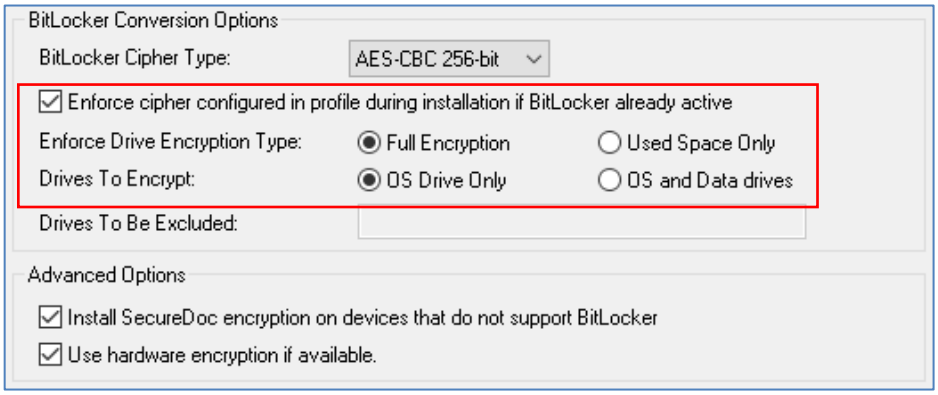
項　目	説　明
BitLocker Encryption:	・Do not use BitLocker encryption デフォルト設定 BitLocker による暗号を使用しません。 ・Enable SecureDoc Pre-boot for BitLocker SecureDoc のプリブート認証を使用します。 SecureDoc プリブート認証によって、細かいパスワードルールでの運用や、ユーザーロック機能、チャレンジ&レスポンス等の機能を使用できます。 また、プリブートネットワーク認証も利用可能です ・Enable Microsoft BitLocker Pre-boot BitLocker が実装している認証をそのまま使用します。 [Authentication method]のプルダウンメニューで、BitLocker の認証方法を選択します。

ここでは、SecureDoc のプリブート認証を使う方法を説明します。

まず、BitLocker の暗号化アルゴリズムを選択します。

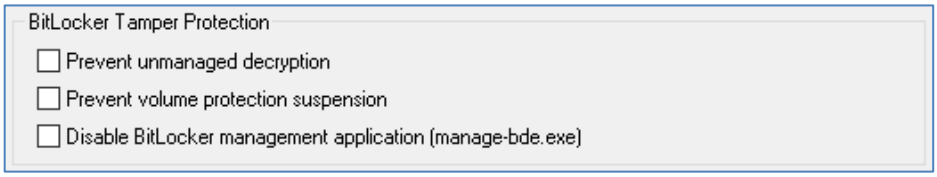


次に、暗号化領域及び暗号化対象のドライブを選択します。



項　目	説　明
BitLocker Conversion Options	
BitLocker Cipher type	プルダウンメニューで、暗号化アルゴリズムを選択します。
Enforce cipher configurated in profile.	BitLocker がすでにアクティブな場合でも、インストール時にプロファイルで設定した暗号を適用します。
Enforce Drive Encryption Type:	暗号化を実行する領域を選択します。
Drives to encrypt:	暗号化を実行するドライブを選択します。
Drives To Be Excluded:	暗号化の対象としないドライブを指定します。
Advanced options	
Install SecureDoc encryption on ….	BitLocker をサポートしていないデバイスの場合、SecureDoc によるソフトウェア暗号を実行します。
Use hardware encryption if available	TCG Opal 等の自己暗号化ドライブを検出した場合、BitLocker によるソフトウェアで暗号化せず、自己暗号化ドライブの暗号化機能を使用します。

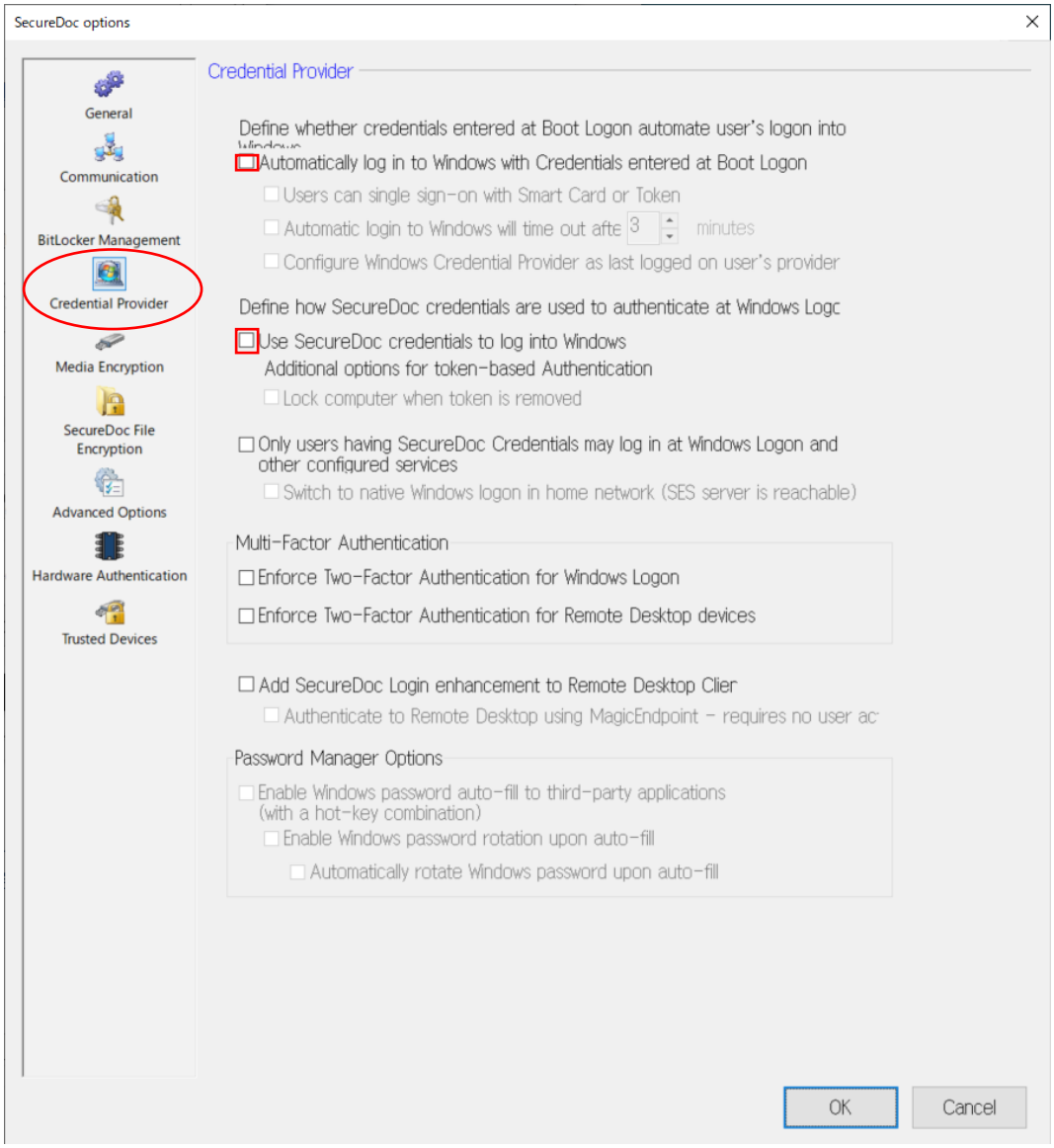
[BitLocker Tamper Protection]では、BitLocker のセキュリティを高めることができます。



項　目	説　明
BitLocker Tamper Protection	
Prevent unmanaged decryption	ユーザーによる BitLocker の削除を禁止します。
Prevent volume protection suspension	デバイスのボリュームレベルで Bitlocker をサスペンドできなくなります。
Disable BitLocker management application (manage-bde.exe)	ユーザーは、manage-bde.exe 実行可能プログラム（BitLocker を無効に変更できる Microsoft ツール）を使用できなくなります。

⑤　次に、左ペインにある[Credential Provider]アイコンをクリックします。

シングルサインオンを有効にする場合は、[Automatically log in to Windows with Credentials entered at Boot Logon]と[Use SecureDoc credentials to log into Windows]にチェックを入れます。



⑥　次に、左ペインにある[Advanced Options]アイコンをクリックします。

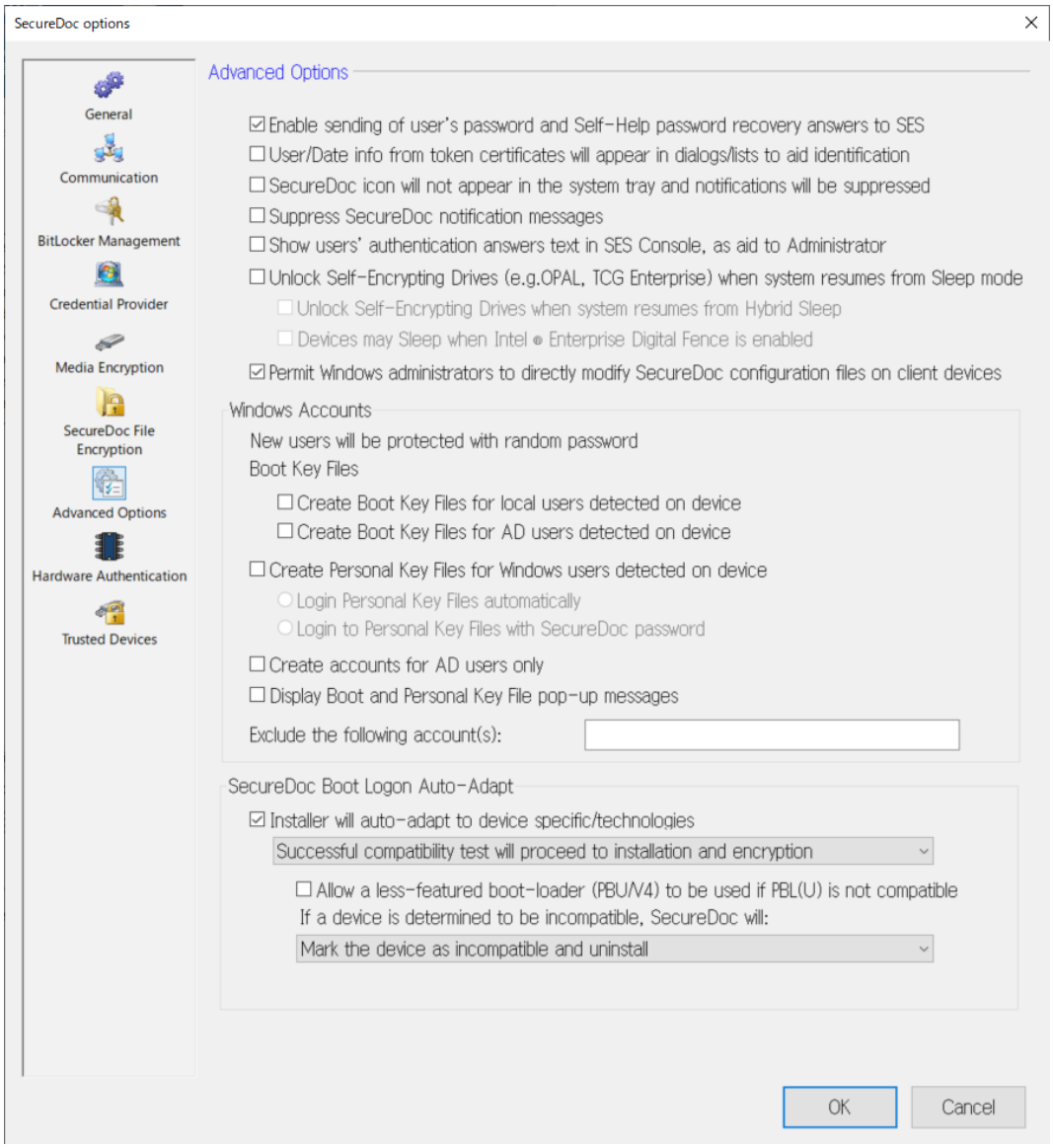
[Installer will auto-adapt to device specific/technologies]にチェックを入れます。プルダウンの設定で、

” Successful compatibility test will proceed to installation and encryption”を選択します。

特別な設定が必要な場合、インストーラーがそれを検知して自動で必要な設定をおこないます。

[If a device is determined to be incompatible, SecureDoc will:]　の設定で、“Mark the device as incompatible and uninstall” を選択します。

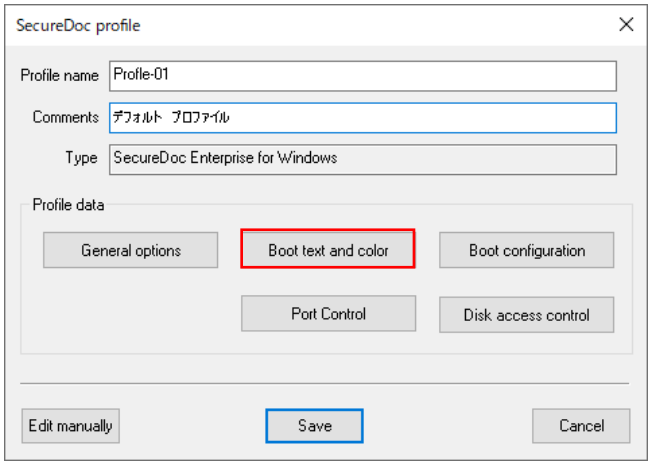
万一、インストールできない場合、SecueDoc をアンインストールして、その情報を SES に送ります。



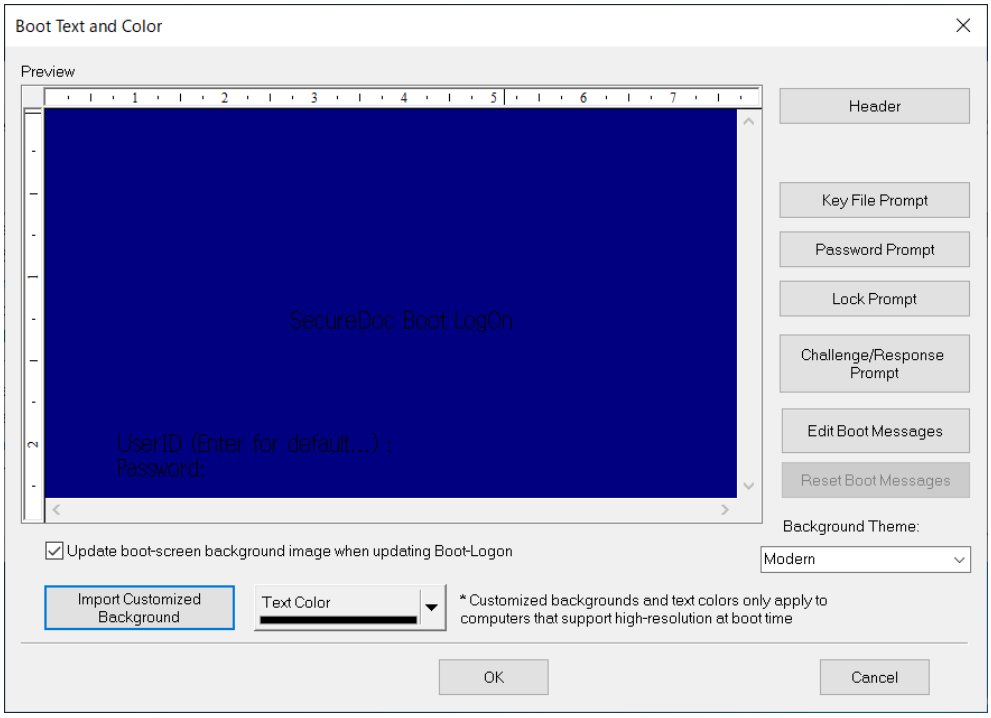
⑦　下部にある<OK>ボタンをクリックし、<General Options>の設定を保存します。

13.2. Boot Text and color の設定

① プロファイル作成トップ画面から、<Boot Text and color>ボタンをクリックします。



② 次の画面が表示されます。



③ 設定を必要とする項目は、<Key File Prompt>、<Password Prompt>、<Lock Prompt> の 3 か所です。

注 クライアントのプロファイルを変更しても、表示される内容が英文に変わらないように設定します。

<Key File Prompt> は、ユーザーID を入力する項目に表示する文字を設定します。

初期設定 User ID (Enter for default...) :

設定例 ユーザーID :

<Password Prompt> は、パスワードを入力する項目に表示する文字を設定します。

初期設値 Password :

設定例 パスワード :

<Lock Prompt> は、続けて ID またはパスワードの誤入力があった場合に表示する文字を設定します。

初期設定

You have incorrectly logged into the computer. If you know your User ID and password, please press Ctrl+Alt+Del and try again. If you don't know your User ID or Password, please contact your Help Desk for assistance.

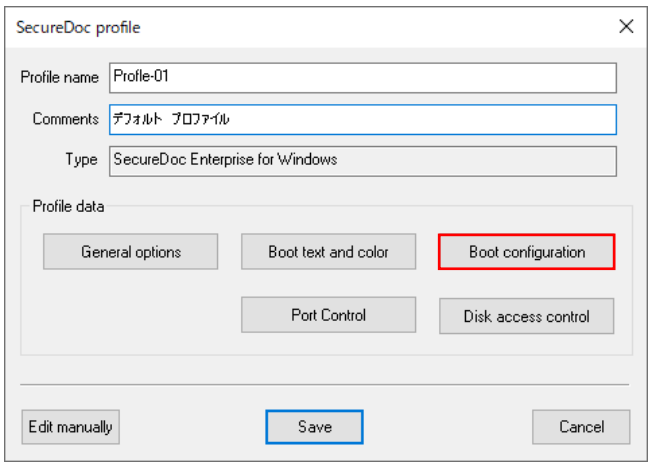
設定例

間違った ID もしくはパスワードが入力されました。
Ctrl + Alt + Del を押して、再起動し、入力し直してください。
もし、パスワードを忘れてしまった場合、社内のヘルプデスクに連絡しださい。
注　紛失時、取得者に持ち主を特定されるような情報の記載は推奨しません。会社名等

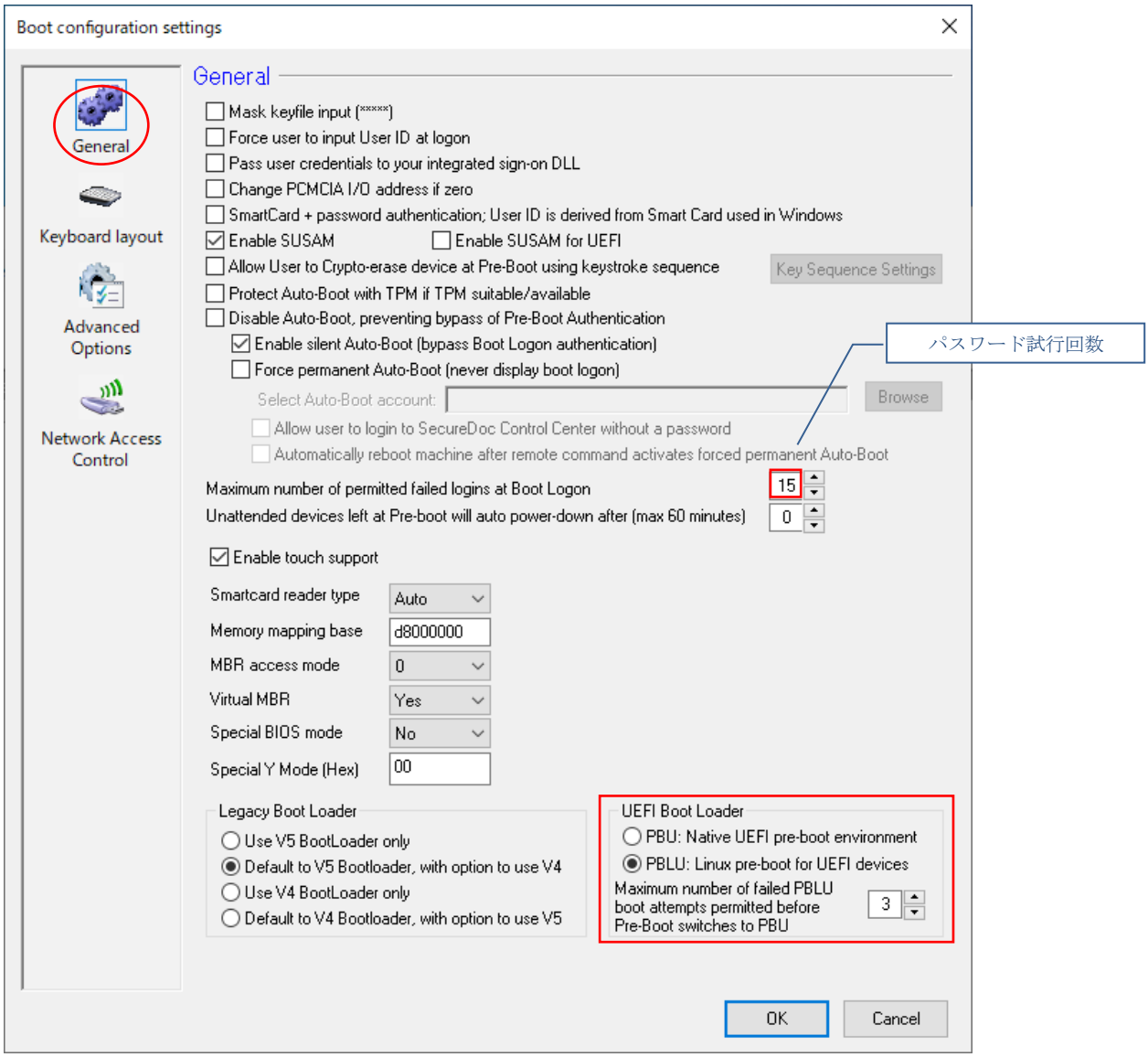
④　設定が完了したら、<OK>をクリックします。

13.3. Boot configuration の設定

① 次に、<Boot configuration>ボタンをクリックします。



② [General]では、[Maximum number of permitted failed logins at Boot Logon]で、パスワード試行回数の上限値を設定します。例えば、5 とすると、連続して 6 回パスワードを間違えるとロックがかかります。
デフォルト設定は 15 です。



UEFI のデバイス向けに、ウィンマジックはプリブート認証プログラム（UEFI Boot Loader）を 2 つ提供しています。

○ PBU: Native UEFI pre-boot environment

◎ PBLU: Linux pre-boot for UEFI devices

注　プリブート認証で、Bluetooth 接続のスマートフォンを使用する場合は、必ず PBLU を選択してください。

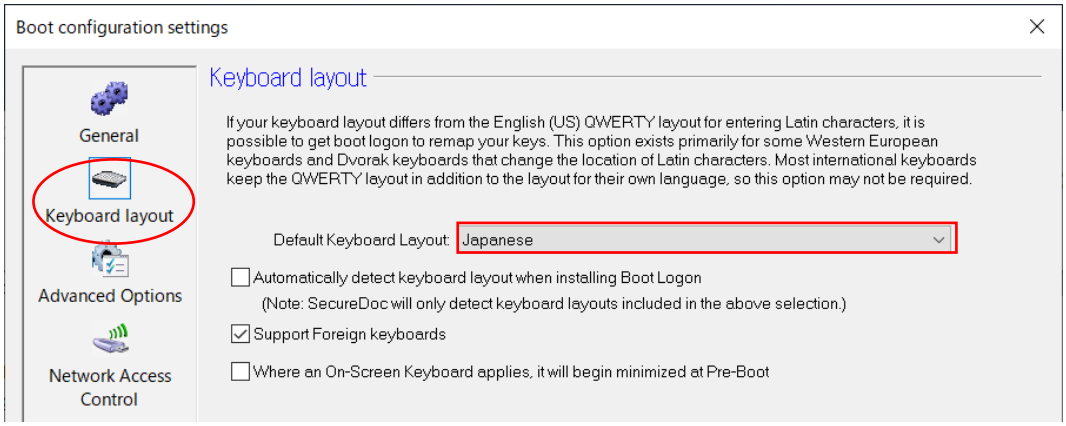
注　プリブートネットワーク認証で、Wi-Fi NIC を使用する場合は、PBLU を選択してください。

※　PBLU では起動を 3 回（デフォルト設定）試し、もし起動できない場合、PBU に切り替えます。

③　次に、[Keyboard layout]アイコンをクリックします。

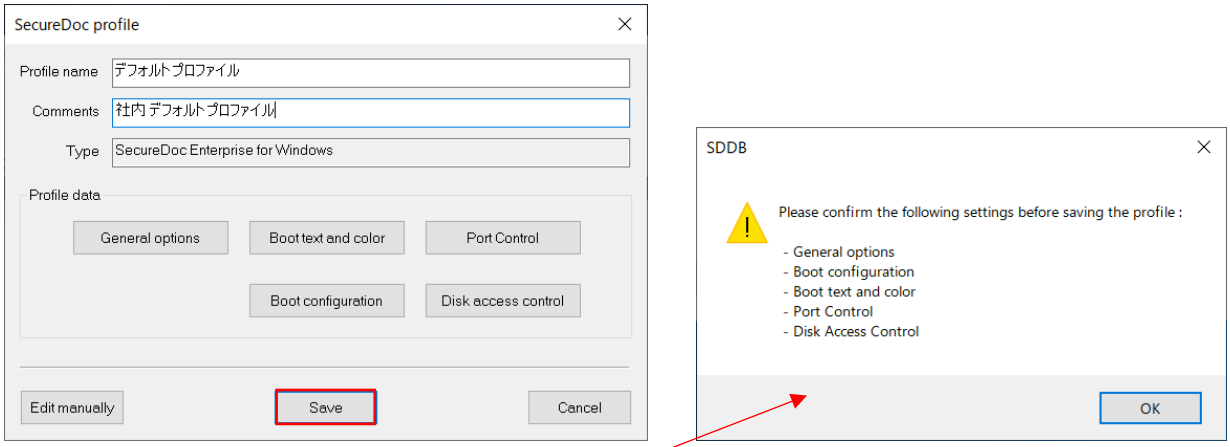
[Default Keyboard Layout]のプルダウンメニューから「Japanese」を選択します。プリブート認証プログラムで、使用するキーボードレイアウトの設定です。

注　英語キーボードが初期設定されているので、必ず変更してください。記号等のレイアウトが異なるので、パスワードに記号を使った場合等、ログインできなくなる場合があります。



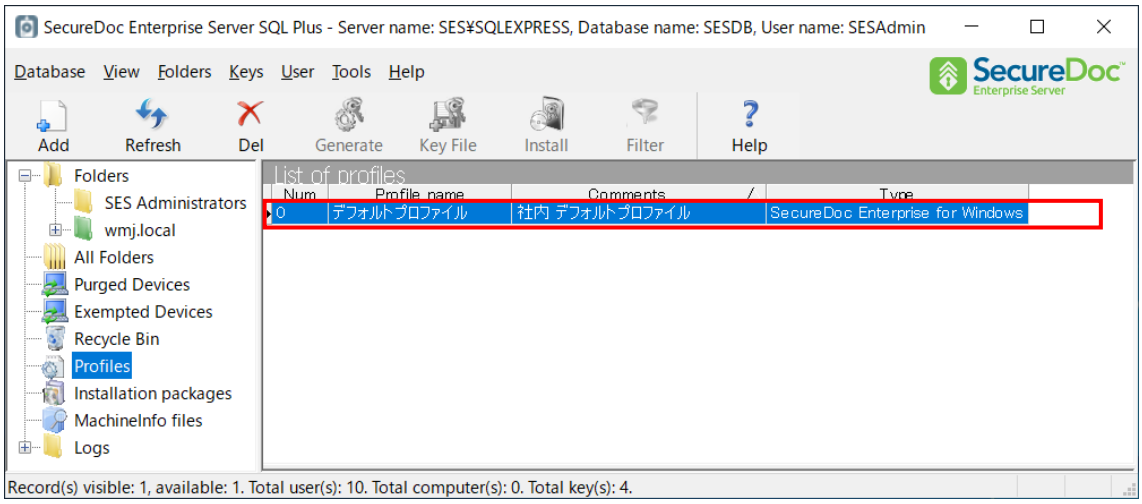
④ <OK>ボタンをクリックします。

⑤ 最後に、<Save>ボタンをクリックして、プロファイルを保存します。

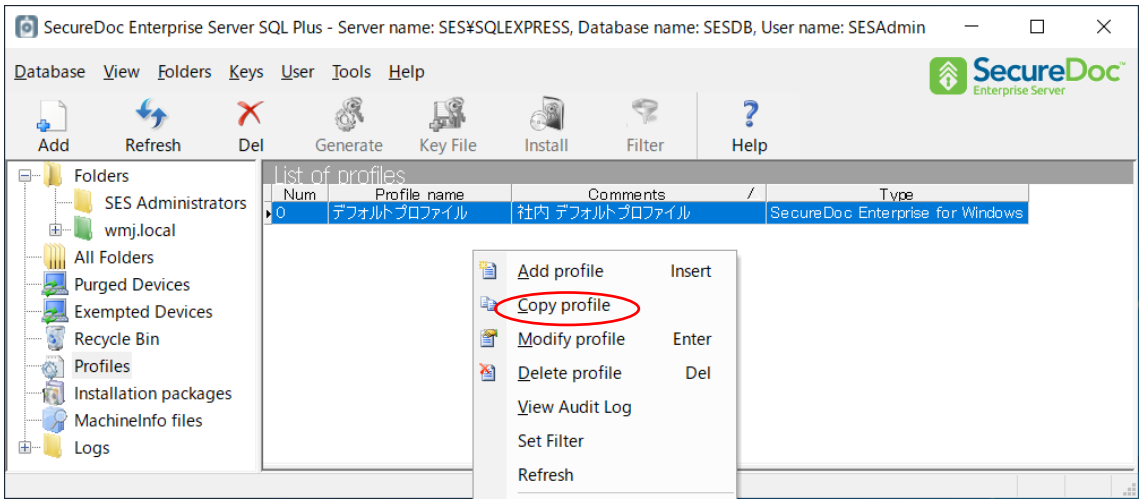


⑥ 設定されていない箇所についてのアラートが右上画面のように表示されますので、<OK>をクリックし、表示された設定画面で、<OK>または<CLOSE>をクリックして、プロファイルを保存します。

⑦ SES 上にプロファイルが作成されたことを確認します。



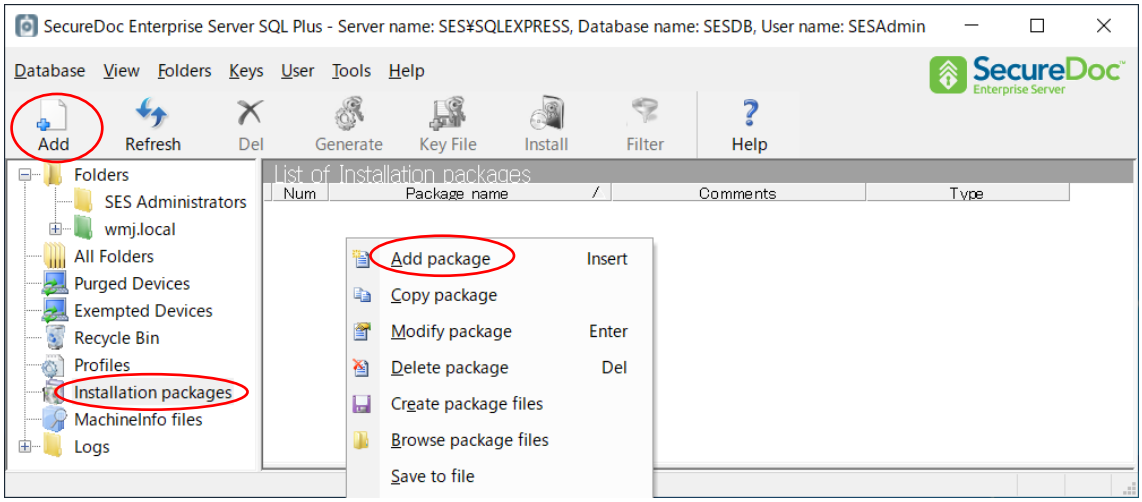
※ 複数のプロファイルを作成する場合、作成済のプロファイルを編集することで簡単に作成できます。
作成済のプロファイルを右クリックして、[Copy Profile]を実行します。[Profile name]に新しいプロファイル名を入力し、必要な項目を編集して保存してください。



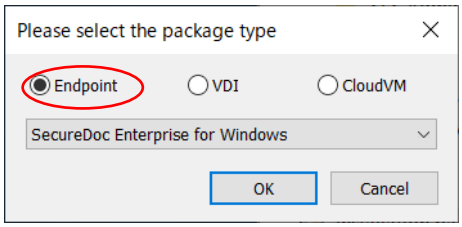
14. Windows 用インストレーションパッケージの作成

「SecureDoc Enterprise for Windows」のライセンスで、プロビジョニンルール「パターン A」および「パターン B」によるインストレーションパッケージの作成方法を中心に説明します。
その他のパターンを使ったインストレーションパッケージの作成方法については、「SecureDoc Enterprise Server Version 9.2 リファレンス マニュアル」をご参照ください。

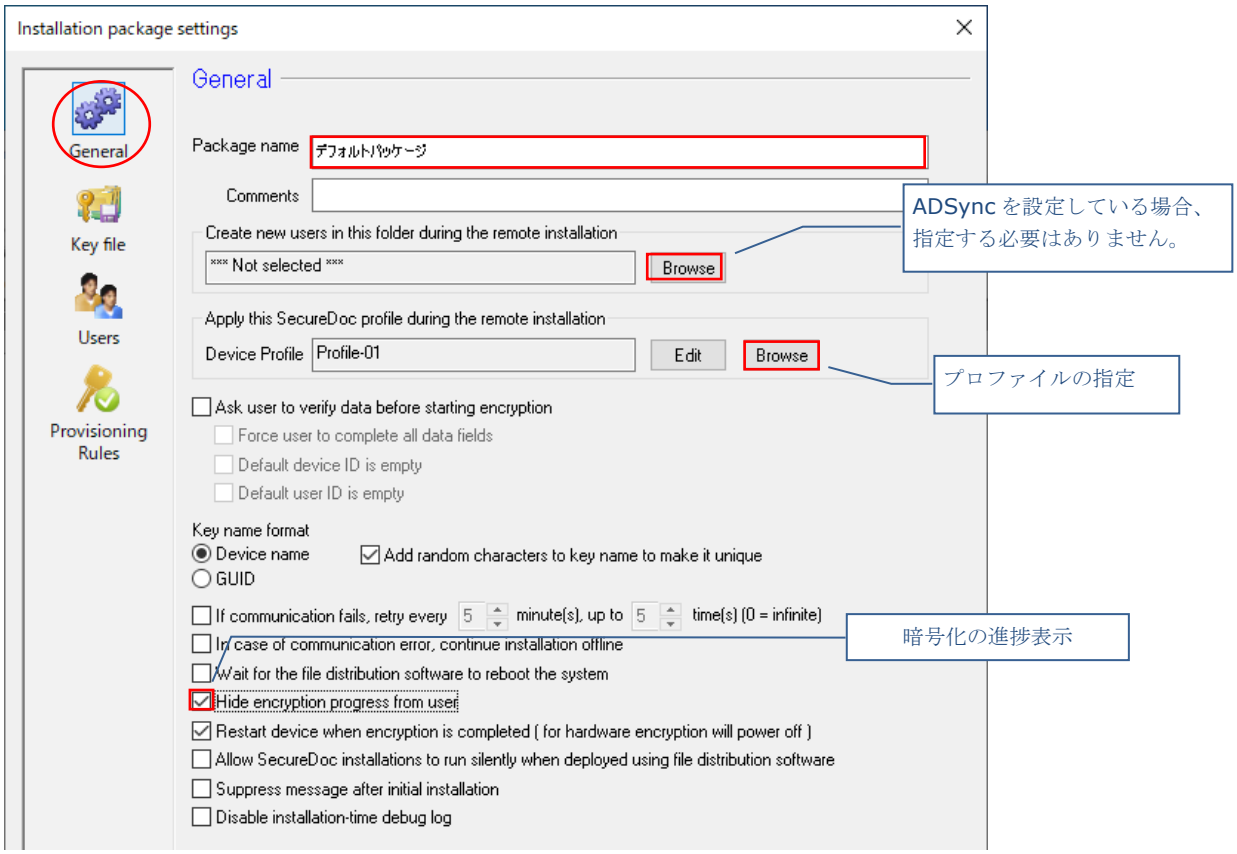
① SES の左ペインより、[Installation packages]アイコンを選択し、上部にある<Add>ボタンをクリックするか、右ペインの上で右クリックし、表示メニューから[Add package]をクリックします。



② [Please select the package type]ウィンドウが表示されますので、[Endpoint]のプルダウンメニューより、「SecureDoc Enterprise for Windows」を選択し、<OK>ボタンをクリックします。



③ [General]欄が表示されますので、[Package name]欄にインストレーションパッケージ名を、必要に応じて[Comments]欄にコメントを入力します。
ADSync を設定していない場合、すぐ下にある<Browse>ボタンをクリックし、インストールによって作成される「オーナーID」、「デバイス」、「暗号鍵」の登録先フォルダを指定します。ADSync を使って OU とその配下の ID をインポートしている場合は、<Browse>ボタンをクリックして登録先フォルダを選択する必要はありません。
次に、[Device Profile]では、<Browse>ボタンをクリックし、事前に作成した SecureDoc クライアントに適用するプロファイルを選択します。



プロビジョニングルールでは、SecureDoc のプリブート認証プログラムで使用するユーザーID（オーナー）は、Windows のサインインに使用された ID と同名の ID を作成するように設定されています。

※　Windows のサインイン ID 名とは異なる SecureDoc のユーザーID を作成する方法については、「SecureDoc Enterprise Server Version 9.2 リファレンス マニュアル」をご参照ください。

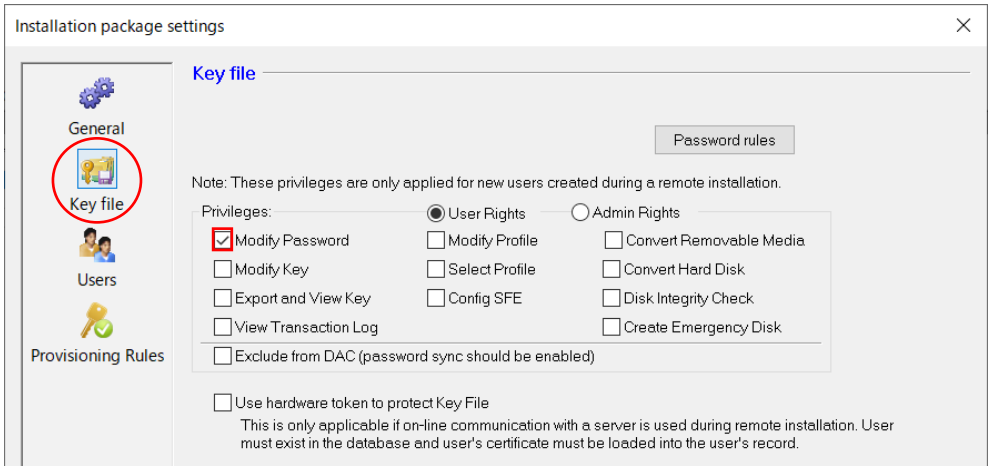
注　暗号化の進捗状況を Windows デスクトップ上にステータスバーで表示する場合、[Hide encryption progress from user]のチェックを外してください。

④　次に、左ペインより、[Key file]アイコンをクリックします。

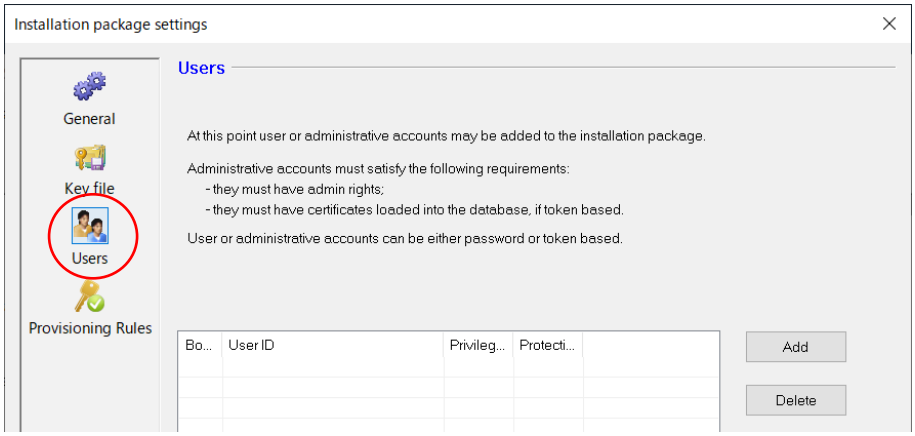
ユーザーID に付与する権限を確認します（グローバルオプションで設定した権限が反映されています）。

変更する場合は、目的の権限にチェックを入れます。

例えば、USB メモリ等の暗号化をするには、[Convert Removable Media]の権限が必要です。

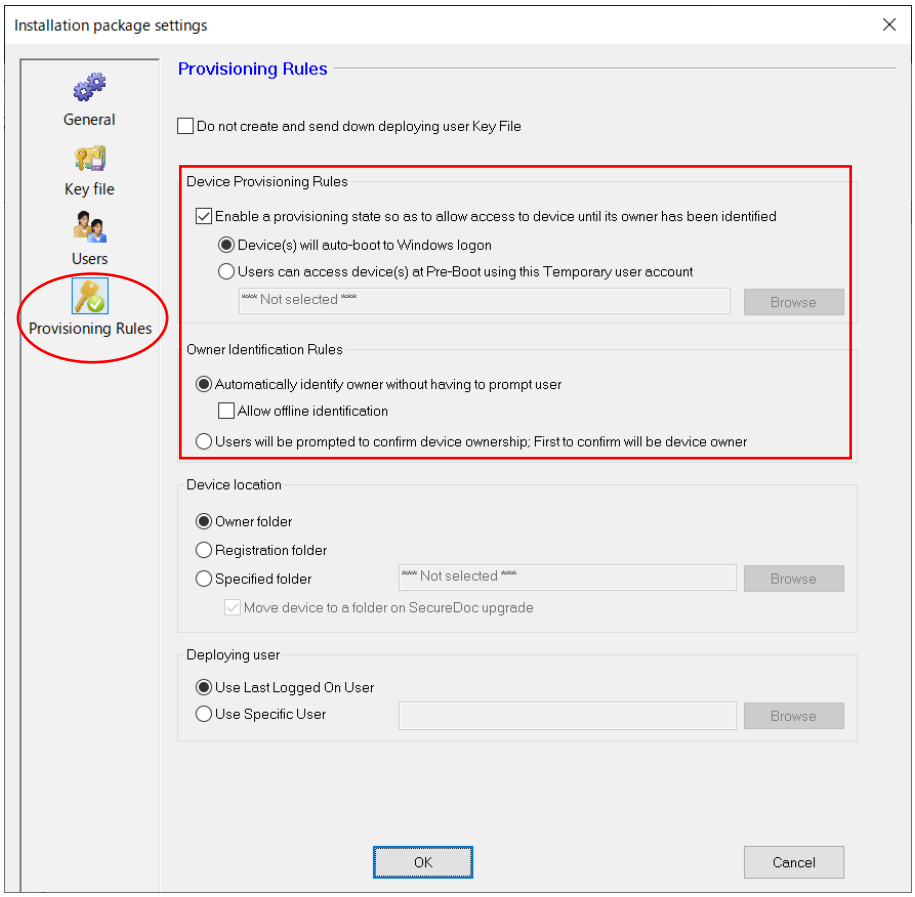


⑤ 左ペインの [Users]アイコンは、管理者 ID をクライアントデバイスに追加する機能です。



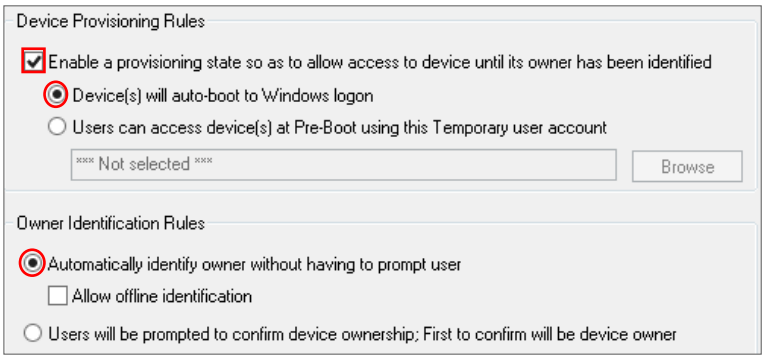
管理者 ID をクライアントに登録する方法は、ここでの設定のほか、より便利なフォルダ単位での方法があります。管理者権限の ID をクライアントに追加したい場合は、「12.8.フォルダの機能を使った管理者 ID の配備や共有鍵の追加」をご使用ください。フォルダの機能を使うと、いつでも管理者 ID の追加や削除が可能です。

⑥ 次に、左ペインにある[Provisioning Rules]アイコンをクリックします。



プロビジョニングルールで必要な設定

「パターン A」の場合：

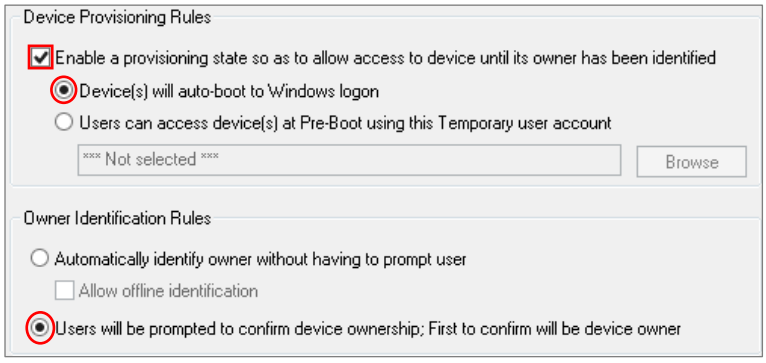


☑ Enable a provisioning state so as to allow to device until……

◎ Device(s) will auto-boot to Windows logon

◎ Automatically identify owner without having to prompt user

「パターン B」の場合：



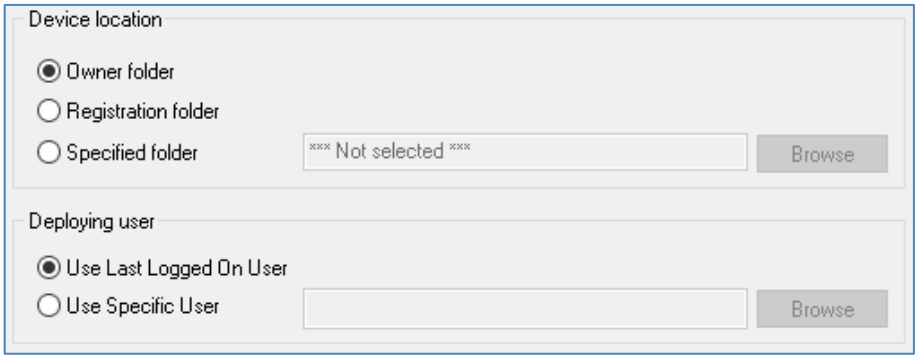
☑ Enable a provisioning state so as to allow to device until……

◎ Device(s) will auto-boot to Windows logon

◎ Users will be prompted to confirm device ownership;……

項　目	説　明
Enable a provisioning state to allow access to device until its owner has been identified	プロビジョニング状態を有効にします。オーナーが確定するまでは、以下のオプションを使って、自動起動あるいは一時ユーザーを使ってデバイスへのアクセスを許可します。
Device(s) will auto-boot to Windows logon option	プリブート認証で、ブートログオン操作を必要とせずに自動起動（オートブート）し、Windows を起動します。
Users can access device(s) at Pre-Boot using this Temporary user account	プリブート認証で、一時的なユーザーID とパスワードを使用してログインするための ID を選択します。オーナーが確定されると、クライアントから一時ユーザーは削除されます。
Automatically identify owner without having to prompt user option.	ユーザーへ操作を要求せずに、自動的にオーナーを設定します。「SecureDoc プライマリアカウントの設定」ダイアログ画面は表示されません。

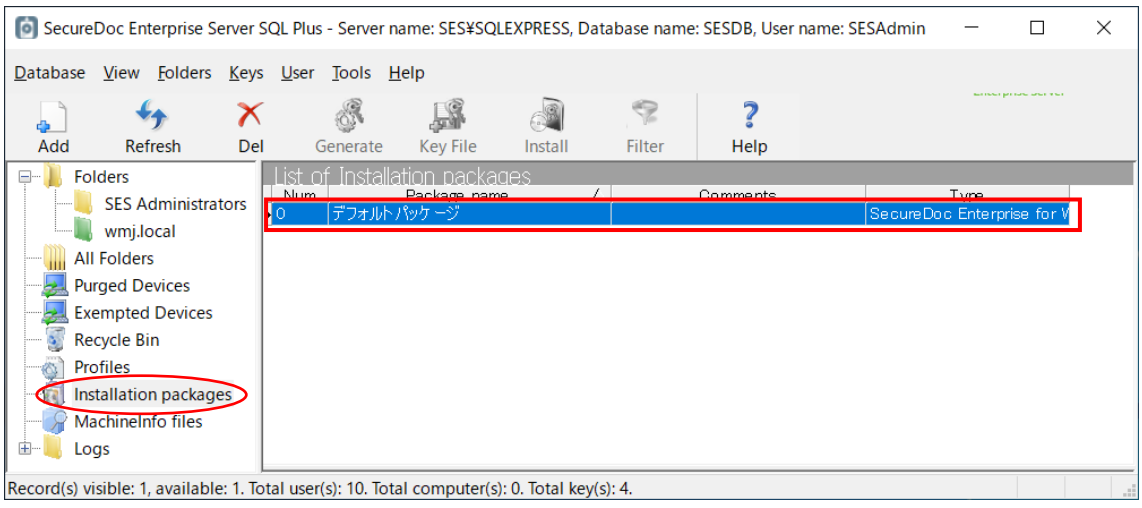
項　目	説　明
Allow offline identification	SDConnex と通信できない環境でも、自動的にオーナーを設定します。
Users will be prompted to confirm device ownership; First to confirm will be device owner	デバイスの所有者を確認するために、「SecureDoc プライマリアカウントの設定」ダイアログ画面を表示します。



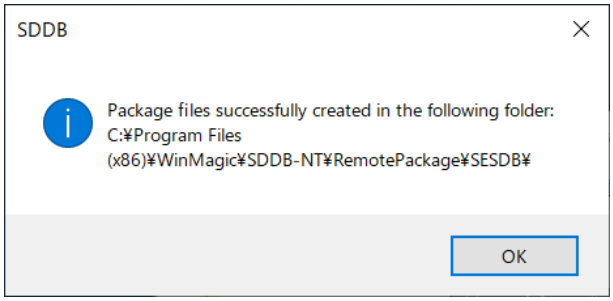
項　目	説　明
Device location	
Owner folder	ADSync を使った場合等、既にユーザーが SES に存在する場合、ユーザーと同じフォルダにデバイスを登録します。通常は、これを選択します。
Registration folder	[General]で指定したフォルダに登録します。
Specified folder	登録先フォルダを指定します。
Deploying user	
Use Last Logged On User	インストール時にログインした Windows ID を展開ユーザーとします。
Use Specific User	展開ユーザーを指定します。

⑦　最後に、<OK>ボタンをクリックし、インストレーションパッケージを作成します。

⑧　SES 上に Windows 用インストレーションパッケージが作成されたことを確認します。



⑨ 次に、作成したインストレーションパッケージを右クリックし、[Create package files]を実行します。作成されると、次のメッセージが表示されます。（フォルダパスは、お客様の環境によって異なります。）



⑩ 作成したパッケージを再度右クリックし、メニューから[Browse package files]を選択すると、パッケージの保存されているフォルダ内が表示されます。

※ 複数のインストレーションパッケージを作成する場合、作成済のパッケージを編集することで簡単に作成できます。作成済のインストレーションパッケージを右クリックして、[Copy package]を実行します。[Package name]に新しいインストレーションパッケージ名を入力し、必要な項目を編集して保存してください。

15. Windows PC へのインストール

15.1. インストーラー実行前の確認事項

以下の内容を必ず確認してから、インストレーションパッケージを実行してください。

☐ Windows のパスワードが設定されていること

プロビジョニングルールでは、Windows サインイン名を使って、ユーザーID を作成しますが、Windows のパスワードが設定されていないと、オーナーを確定できず、ID を作成できません。

☐ TCG Opal ディスクの場合、「HDD パスワード」あるいは「SID（Block SID）」を設定していないこと

HDD パスワードあるいは Block SID が設定されていると、Opal として動作させるためのアクティベーションができません。

☐ BitLocker の設定を確認してください。

SecureDoc によるソフトウェア暗号を実行するインストレーションパッケージでは、BitLocker が有効になっていると、インストールは失敗します。BitLocker で暗号化済のデバイスにインストールする場合は、プロファイル内の [BitLocker management]の設定が必要です。

☐ PC の時計を正確にあわせてください。

SecureDoc インストール後、日付と時刻の変更操作は、不正な行為として扱われ、キーファイルはロックされます。（海外との時差は考慮されています）

☐ 使用中の PC を暗号化する場合、SecureDoc のインストール前にデータをバックアップし、ドライブのエラーチェックと、HDD の場合はデフラグも併せて実行することを強く推奨します。

☐ スリープ、休止の設定について

暗号化中、電源管理によって PC（HDD/SSD）が停止しないようにしてください。

☐ インストールする PC のディスク空き容量の確認

10% 程度空き容量があることを確認してください。

☐ サーバー上で SDConnex サービスが起動しているかを確認してください。

☐ クライアントと SDConnex がインストールされているサーバーが通信できる状態にあること

☐ デバイスから USB メモリ等のストレージ機器を取り外してください。

15.2. 制限事項

☐ ID/パスワードには、円マーク と バックスラッシュ を利用できません。

ブートログオンを使ったプリブート認証で、円マーク と バックスラッシュ は入力できません。

☐ UEFI デバイスの場合は、_（アンダーバー）もご利用になれません。

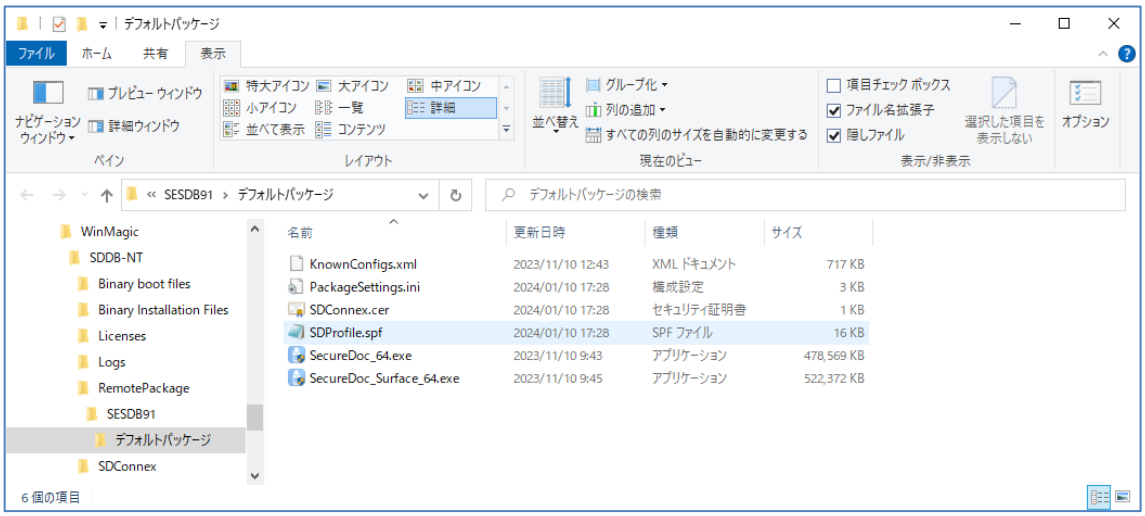
☐ SecureDoc をインストール後、UEFI / BIOS の日付と時刻は、正しく保つようにしてください。

通常、UEFI / BIOS の日付と時刻は、Windows の設定と同期していますが、時刻変更の操作は、不正な行為として扱われ、キーファイルはロックされます。（海外との時差は考慮されています）

15.3. SecureDoc クライアントのインストール手順

インストールには、Windows の管理者権限が必要です。インストールのプロセスで、OS は再起動されますので、作業中のデータは保存し、実行中のプログラム等を終了してからおこなってください。

① 「14. Windows 用インストールパッケージの作成」で、作成したインストレーションパッケージに含まれるファイルを、フォルダごと、クライアント PC の任意の場所にコピーします。



② インストール実行前に、次のファイルが、含まれていることを確認してください。

ファイル名	種類	
KnownConfig.xml	XML ドキュメント	デバイス特有の設定が必要な既知情報がある場合、自動で設定を反映させます。
PackageSettings.ini	構成設定	
SDConnex.cer	セキュリティ証明書	SDConnex と通信するために必要です。
SDProfile.spf	SPF ファイル	
SecureDoc_64.exe	アプリケーション	Windows 64bit 用インストーラー
SecureDoc_Surface_64.exe	アプリケーション	Surface 用インストーラー

注 Microsoft Surface デバイスにインストールする場合の注意：
Microsoft Surface Pro 1、2、または Surface Book へのインストール:
SecureDoc_64.exe を使用してください。
Microsoft Surface Pro 3、4、Surface Pro 2017 または Surface Book 2 へのインストール:
SecureDoc_ Surface_64.exe を使用してください

③ 「SecureDoc_64.exe」を管理者権限アカウントで実行します。インストールが始まりますので、しばらく待ちます。

④　OS によるインストールについての確認を求められたら、<はい>をクリックします。

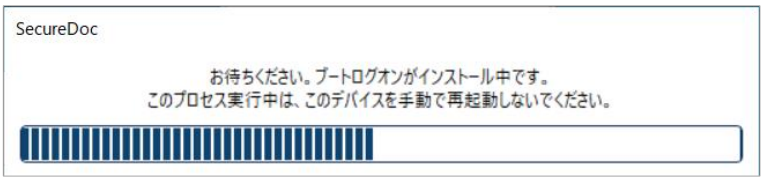
注　プログラムのインストール中に SDConnex との通信に障害が発生すると、次の画面が表示されます。

SDConnex サービスの稼働状態やクライアント PC と SDConnex がインストールされているサーバーの通信の状況を確認してください。通信の問題を解決できたら、<送信>をクリックしてください。再度通信を試みます。この画面で、<キャンセル>をクリックすると、WinMagic SecureDoc の初期設定が中断されます。

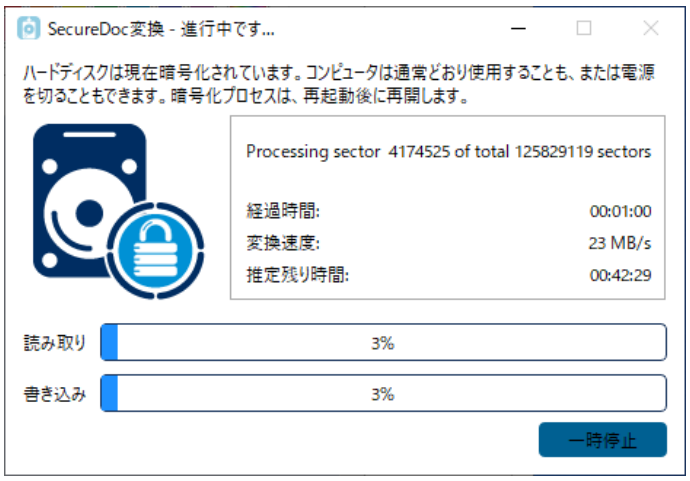
注　中断した場合でも、SecureDoc のプログラムはインストールされた状態であるため、再インストール前に、SecureDoc をアンインストールしてください。この時点では暗号化やプリブート認証プログラムのインストールはおこなわれていないため、Windows のコントロールパネルの「プログラムのアンインストール」からアンインストールできます。

注　<更新>は、クリックしないでください。
クリックすると、「SecureDoc の登録フォーム」（SDForm）が起動します。通常のインストールでは、ユーザーがこの画面で操作をする必要はありません。
SDForm は PC の情報やユーザーID をユーザー自身が入力する場合に利用します。
ここで、ユーザーID やコンピューター名を手入力し、<OK>をクリックすると、インストールの再開を試みます。SDConnex と接続できると、インストールが再開されますので、エンドユーザーがインストールを実施している場合、システム管理者が望まない ID が設定される可能性があることに注意してください。

⑤ SDConnex と正常に通信がおこなわれると、ブートログオンがインストールされます。インストール後、自動的に OS が再起動します。



⑥ OS 再起動後、自動的に暗号化が開始されます。



暗号化中であっても、シャットダウンすることは可能です。
（プロファイル設定で、No recovery(faster)を指定した場合を除く）
デバイスをシャットダウンした後の起動、あるいは「休止」、「スリープ」状態から復帰した場合、暗号化の途中から再開されます。

注 プロファイル設定で、[No recovery(faster)]にチェックを入れている場合は、暗号化途中で電源が切れないように十分注意してください。

⑦ 暗号化状況の進捗を確認する場合は、タスクトレイの SecureDoc のアイコンにカーソルを合わせます。
インストレーションパッケージの[General]-[Hide encryption progress from user]のチェックを外している場合は、暗号化の進捗状況が画面に常に表示されます。

⑧ 暗号化が完了すると、60 秒後に、再起動します。

※ TCG Opal 自己暗号化ドライブの場合は、ハードウェア仕様に基づき、シャットダウンになります。

⑨ プロビジョニングルールの「パターン B」によるインストレーションパッケージでは、「SecureDoc プライマリアカウントの設定」画面が表示されます。

⑩ デバイスの所有者の場合は<OK>をクリックします。デバイスオーナーが確定します。
デバイスの所有者ではない IT 担当者やキッティング業者がインストールしている場合は、<後で>をクリックします。再起動すると、再度、この画面が表示されるので、デバイスの所有者以外がインストールしている場合は、<後で>をクリックします。

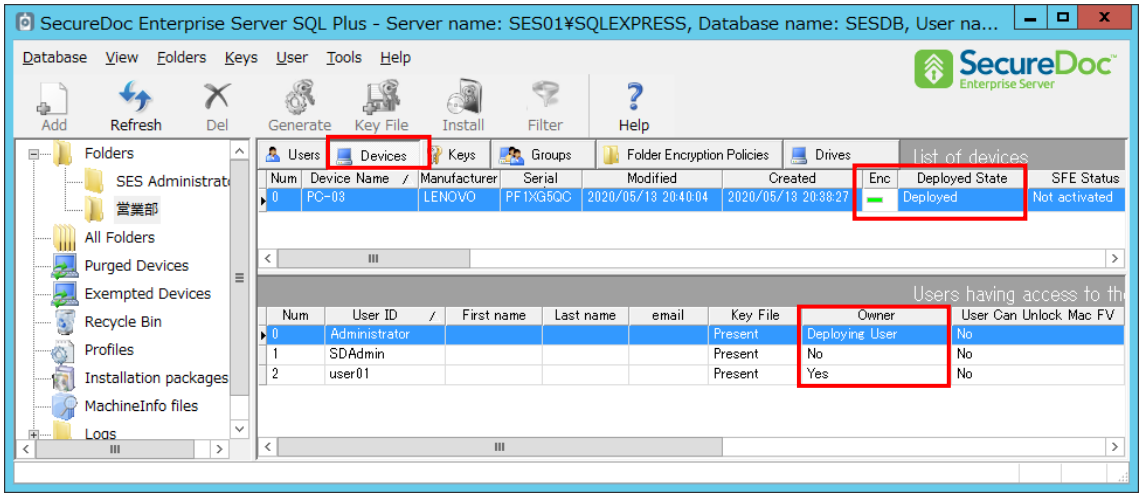
⑪ デバイスの起動時に、プリブート認証画面が表示されるようになります。
環境により、表示される画面が異なる場合があります。

※ プロビジョニングルールの「パターン B」によるインストールで、<後で>をクリックした場合、デバイスオーナーが確定しないため、<OK>をクリックするまでプリブート認証画面は表示されません。

⑫ プロファイルでシングルサインオンの設定がされている場合、自動で設定がおこなれます。

⑬ クライアントに SecureDoc がインストールされると、SES 上にキーファイル、デバイス、鍵が登録され、暗号化が完了すると、次の画面のように SES の Device リストの「Enc」のコラムが緑色になります。

「Deployed Status」のコラムで、オーナーが確定し、配備が完了したデバイスは、Deployed（配備済）と表示されます。デバイス一覧からデバイスを選択し、「Owner」のコラムで、ステータスが Yes となっている User ID がオーナーです。

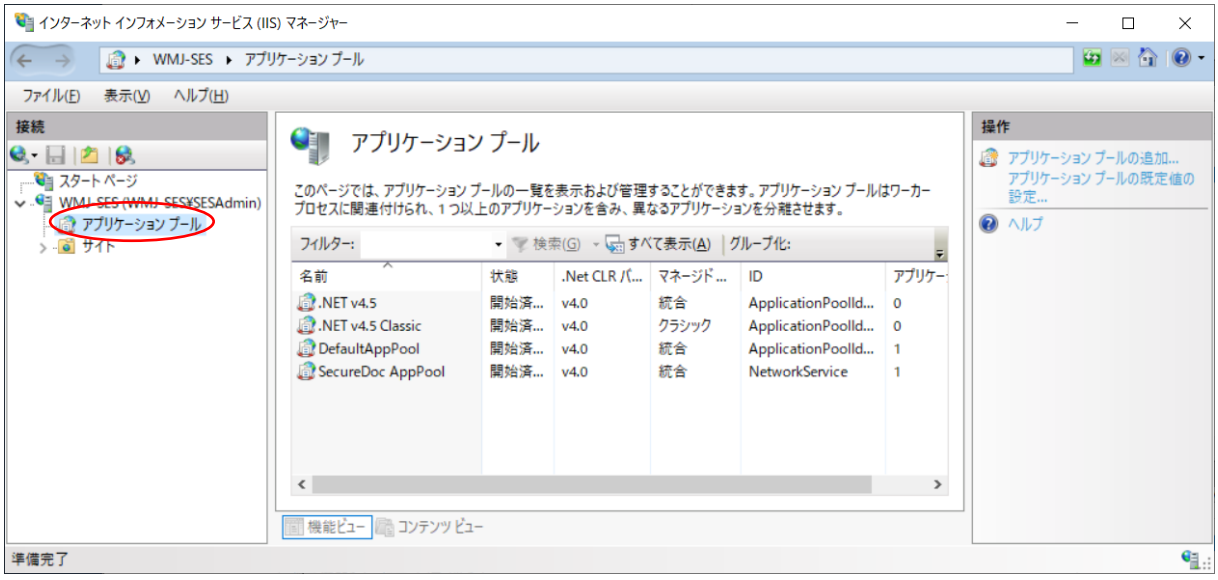


16. SES Web の設定

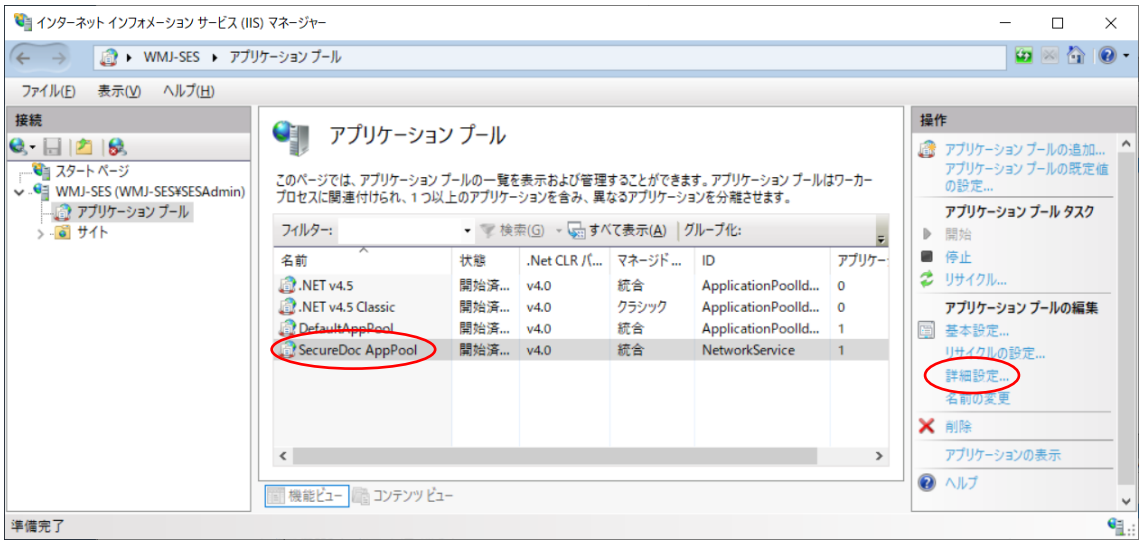
SES Web (SDWeb とも呼ばれる) コンソールは、SES の基本機能の他に、SES コンソールには無いレポート機能があります。

① [スタート] > [Windows 管理ツール] > [インターネットインフォメーションサービス（IIS）マネージャー] を実行します。

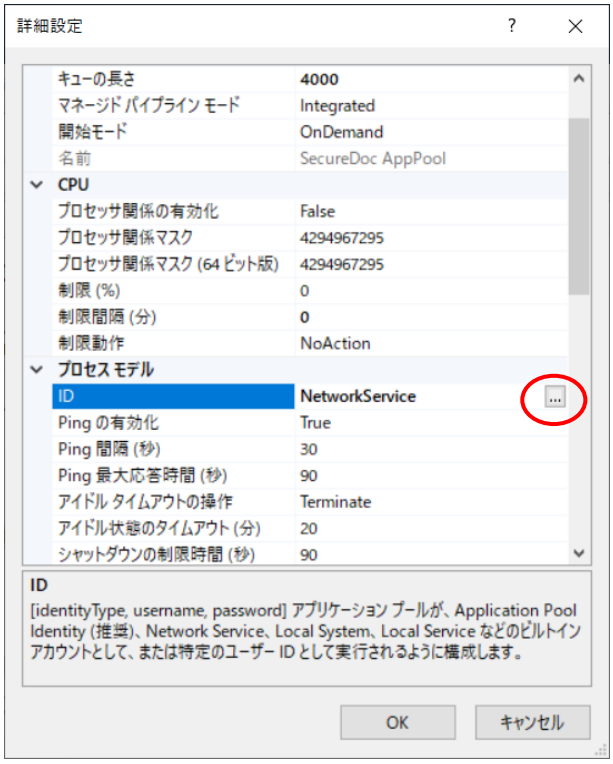
② 左側のペインからサーバーツリーを展開して、[アプリケーションプール]をクリックします。



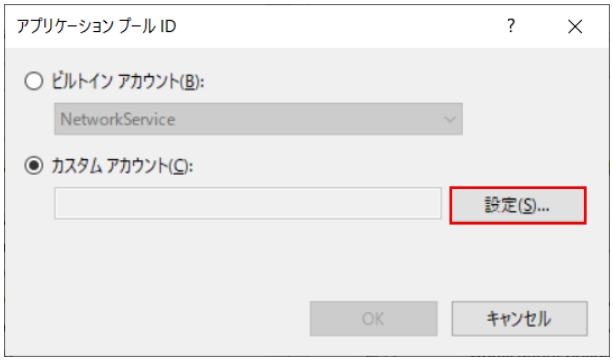
③ SecureDoc AppPool を選び [詳細設定]をクリックします。



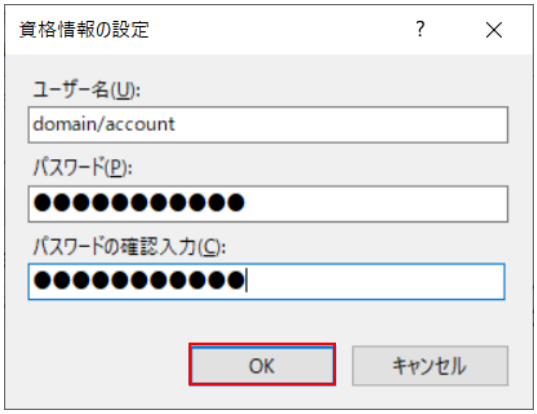
④ [詳細設定]をクリックして、表示された画面のリストから[ID]を探し、右側の 3 つのドットがあるボタンをクリックしてください。



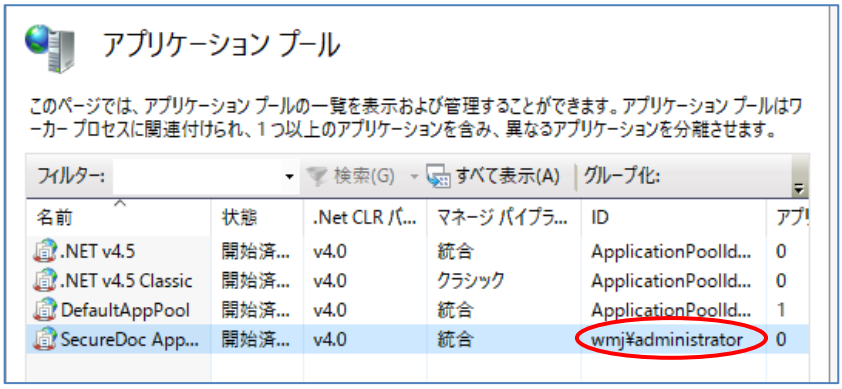
⑤ カスタムアカウントのラジオボタンを選び、<設定>をクリックします。



⑥ サービスアカウント（SDConnex の実行に使用されたのと同じアカウント）の認証情報を入力し、<OK>をクリックします。



⑦ [アプリケーションプール]画面で、アカウントが設定されていることを確認します。



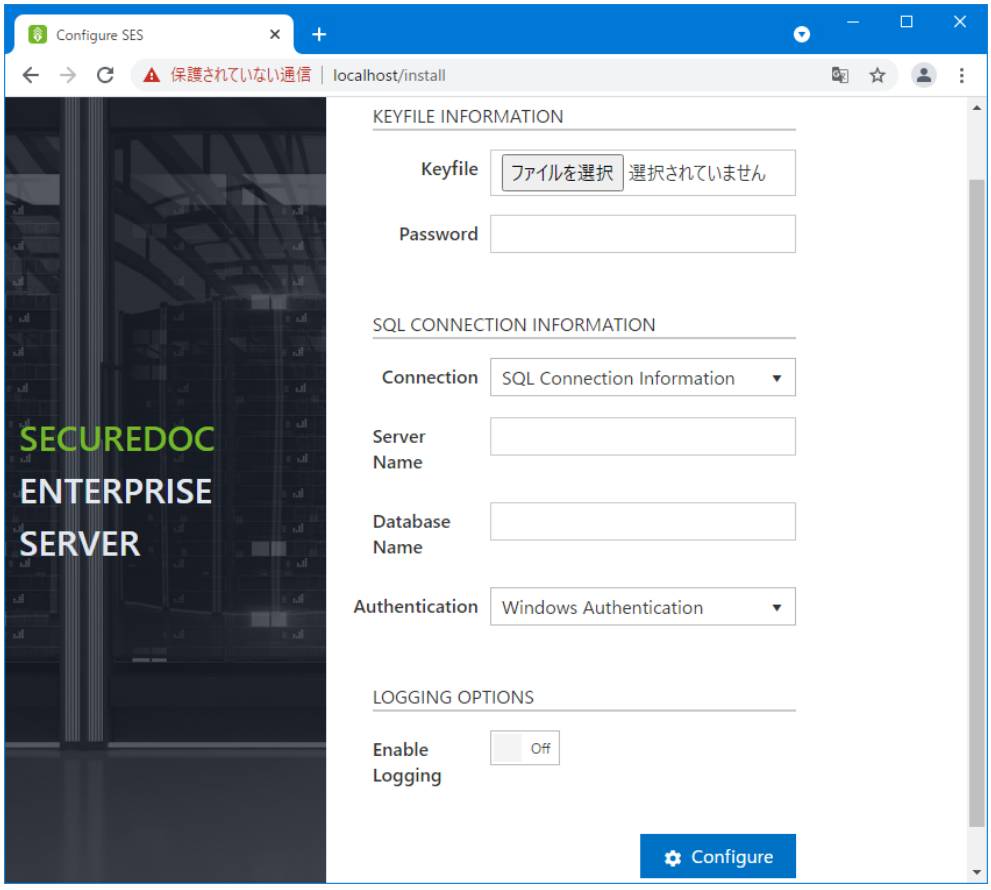
⑧ 左ペインのサーバー名をクリックし、右ペインにある操作メニューから IIS サーバーを再起動します。

⑨ 再起動後、SecureDoc アプリケーションプールが "開始済み" となっていることを確認します。

⑩ 次に、SES Web が SES データベースに対してどのように認証されるのかを定義します。

⑪ ブラウザで、「https://localhost」を開きます。SES Web が実行されているサーバーでブラウザを直接開く必要があります。他のデバイスからアクセスできません。

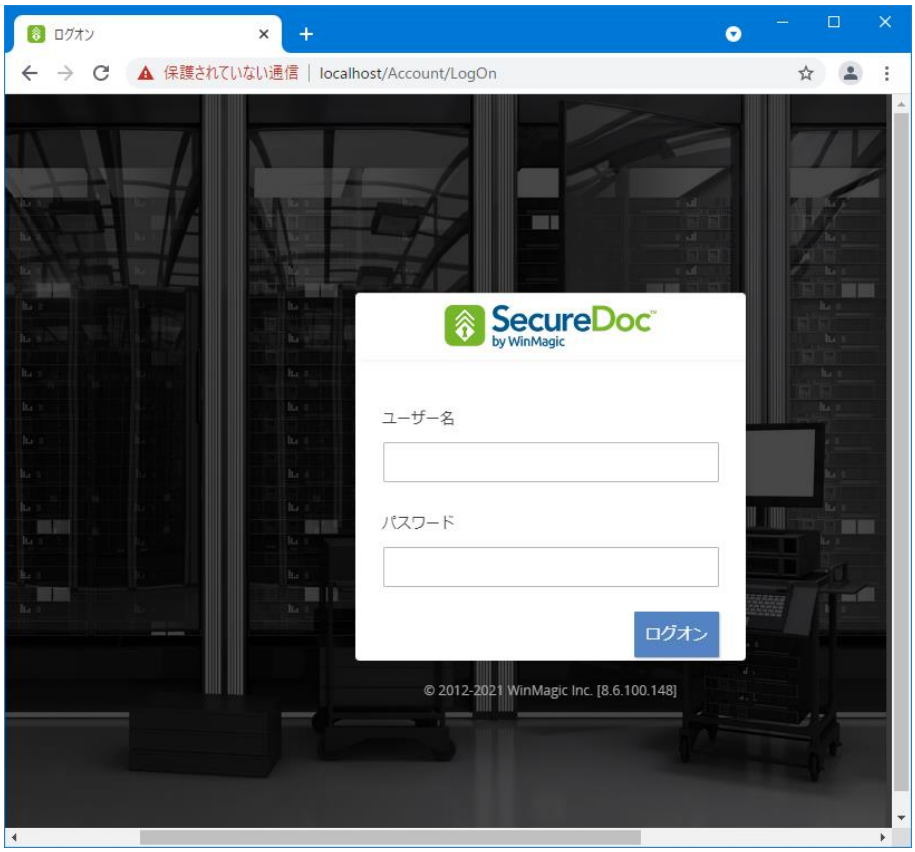
ブラウザは、この構成プロセスが以前に実行されているか否かを自動的に判断し、次の画面に示すように「https://localhost/Install」にリダイレクトします。



注 使用するブラウザは、IE では動作しません。Edge、Chrome、Firefox のいずれかをお使いください。

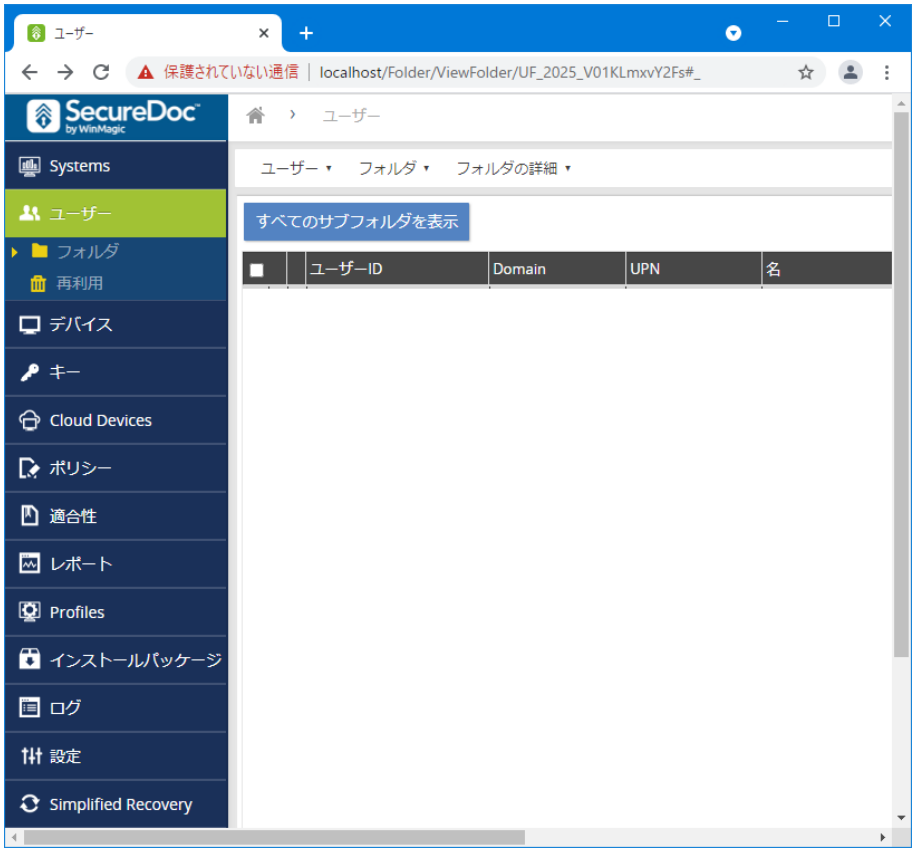
項　目	説　明
KEYFILE INFORMARION	
Keyfile	SES インストール時に作成した Keyfile の場所を指定します。
Password	Keyfile 作成時に設定したパスワードを入力します。
SQL CONNECTION INFORMATION	
Connection	“SQL Connection Information” のままにします。
Server Name	SQL Server を実行しているサーバー名を入力します。 例：　SES01¥SQLEXPRESS
Database Name	SES データベース名を入力します。
Authentication	ドロップダウンで、SQL 認証 ('sa' アカウント) を使用するか、Windows の資格情報を使用するかを選択します。 Windows の資格情報を使用する場合は、アプリケーションプールに設定した情報が使われます。 SQL 認証を使用する場合は、ユーザー名とパスワードを入力します。
LOGGING OPTION	
Enable	必要に応じてログ機能を有効にします。

⑫　設定後、<Configure>をクリックします。正しく設定されると、次の画面が表示されます。



⑬　SES のインストール時に設定した管理者用キーファイルのユーザーID とパスワードをそれぞれ[ユーザー名]欄、[パスワード]欄に入力し、<ログオン>ボタンをクリックします。

⑭　ログオンに成功すると、次のような画面が表示されます。



⑮　ログアウトする場合は、画面右上にある[ログアウト]メニューをクリックします。

一定期間、操作がない場合は、ユーザーをログアウトしてログイン ページにリダイレクトします。

デフォルト値：15 分

17. Appendix

17.1. プリブート認証の利用方法について（補足）

SecureDoc のプリブート認証画面には、「ID（Key File）」と「パスワード」の入力フィールドがあります。設定により、オーナーID のみが登録されているデバイスと、複数の ID が登録されているデバイスでは、以降の違いがあります。

カーソルの位置について

デバイスにユーザーが 1 人（ID が 1 つ）のみ登録されているデバイスでは、プリブート認証画面でのカーソル位置は「パスワード」フィールドにあり、ユーザーが 2 人以上登録されている場合、カーソルの位置は「ID（KeyFile）」のフィールドにあります。

例えば、プロビジョニンルールで、オーナーの ID のみが展開されたデバイスでは、カーソルの位置は「パスワード」フィールドにありますが、管理者ユーザーを追加した場合は、デバイスに 2 つの ID があるので、カーソル位置は「ID（KeyFile）」のフィールドにあります。

ID の入力について

プロビジョニンルールで登録されたオーナーは、「パスワード入力」だけでログインできます。
複数の ID が登録されているデバイスでも、プロビジョニンルールで登録されたオーナーは、ID を入力せずに、エンターキーや Tab キーで、ID フィールドからパスワードフィールドに移動し、パスワード入力だけでログインできます。
※　ID の入力を必須とする設定も可能です。

パスワード試行回数の上限値について

プロファイル設定の[Maximum number of permitted failed logins at Boot Logon]で、パスワード試行回数の上限の初期値は 15 回に設定されています。設定した回数に関係なく、3 回ログインに失敗すると、次のメッセージが表示されます。（表示されるメッセージが異なる場合があります。）

「コンピュータに正しくログインしていません。ユーザーID とパスワードが
分かっている場合は、Ctrl+Alt+Del キーを一緒に押して、もう一度お試しください。
ユーザーID またはパスワードが分からない場合は、ヘルプデスクに連絡して指示に従ってください。」

画面下の<リブート>ボタンを押すか、Ctrl+Alt+Del キーで、再起動が必要です。再起動を繰り返し、誤入力の累計で、パスワード試行回数の上限値に達すると、ユーザーのキーファイルはロックされます。ロックされた場合、SES 管理者に連絡して、チャレンジレスポンスを使って解除をおこないます。画面に表示されたヘルプデスクとは、SES 管理者のことを示しています。

注　失念したユーザーID またはパスワードの確認や、ロックされたデバイスの解除を希望されて、ウィンマジックにご連絡いただいても、お客様の SES で作成された DB や暗号鍵をお預かりしていないため、対応することは不可能です。

17.2. SDConnex 設定・機能一覧

General

項　目	説　明
Keyfile	
Keyfile path:	キーファイルを指定します。
Keyfile Password:	キーファイルのパスワードを入力します。
Database	
Server¥Instance:	SQL のインストールされているサーバー名とインスタンスを指定します。
Database:	接続するデータベース名を入力します。
Mirror(optional):	データベースのミラー。 注：マイクロソフト社によると、この機能は、Microsoft SQL Server の将来のバージョンで削除される予定です。 https://docs.microsoft.com/ja-jp/sql/database-engine/database-mirroring/database-mirroring-sql-server?view=sql-server-ver16
◎ Windows Login	Windows 認証モードで、SQL に接続します。
○ SQL Server Login	SQL Server 認証モードで、SQL に接続します。
Service	
☐ PBConnex Autoboot Service	プリブートネットワーク認証で、オートブートを利用する場合、オンにします。
☐ Schedule Tasks	一ヶ月以上前の SDConnex パフォーマンス統計情報を削除するタスクをスケジュールする場合にオンにします。
Logging	
☐ Log Events	イベントをログに記録します。
☐ Enable Detailed Trace to Folder	詳細ログを取得する場合、オンにします。 通常、オンにする必要はありません。サポートから詳細ログの要求があった場合に利用します。

Communication

項　目	説　明
PC SecureDoc Client Communication	
Service Port Number:	SecureDoc クライアントと SDConnex が通信に使用するポート番号
Use restricted Ports (1024)	1023 以下のポート番号を使用する場合、オンにします。
Service IP Address:	SDConnex のサービスを起動するサーバーの IP アドレス
Maximum Concurrent Session	最大同時セッション デフォルト設定は 100 です。 （通常、設定変更する必要はありません。） 20,000 台以上のクライアントデバイスの場合、最小 50、最大 100 を推奨します。
Receive Request Timeout:	受信リクエストのタイムアウト （通常、設定変更する必要はありません。） タイムアウトしてセッションを切断する前に、SDConnex がクライアント デバイスからの要求を受信するまで待機する時間を入力します。
Send Response Timeout:	送信レスポンスのタイムアウト （通常、設定変更する必要はありません。） タイムアウトしてセッションを切断する前に、SDConnex がクライアント デバイスに応答を送信するまで待機する時間を入力します。
Checked for Active Commands every	SDConnex がアクティブなコマンド（例えば、キーファイルの更新など）をチェックする頻度を入力します。指定された間隔で、SDConnex は、コマンドが実行されたクライアントデバイス上の SecureDoc エージェントをウェイクアップします。
Quarantine Timeout	疑わしいデバイスが隔離タイムアウトになる時間を入力します。 疑わしいデバイスとは、キーまたはデバイス情報がデータベースにないにもかかわらず、SDConnex への接続を何度も試みるデバイスのことです。隔離中、そのデバイスからの接続試行を無視します。
Busy State Sessions Count:	ビジー状態のセッション数 （通常、設定変更する必要はありません。）
Idle State Sessions Count:	アイドル状態のセッション数 （通常、設定変更する必要はありません。）
Keyfile Update Task Sleep Interval	キーファイル更新タスクのスリープ間隔 （通常、設定変更する必要はありません。）
Remote Installation	
User existence is required	SES DB に存在するユーザーのみにインストールを許可します。 AD Sync や CSV で SES にインポートした ID と、一致した Windows サインイン名のクライアントのみに SecureDoc のインストールを許可することができます。 クライアントインストール実行時に、SES DB にユーザーが存在しない場合、インストールは許可されず中止されます。 これにより、意図しない ID が作成されるのを防げます。
Use password from user record for existing users	キーファイルのイニシャルパスワードとして、SES DB のユーザーに記録されたパスワードを使用する場合、オンにします。SES からユーザーをクライアントに配信する際等に使われます。
Move devices into Recycle Bin in case of reinstallation of SecureDoc	SecureDoc がクライアント デバイスに再インストールされた場合、SES に既に存在するデバイスを Recycle Bin に移動します。 これにより、SES DB でデバイスが重複するのを防ぎます。

Alerts

項　目	説　明
☐ Enable Alerts	アラートを有効にします。
Email configuration	
SMTP Sever:	SMTP サーバー名を入力します。
Port Number:	ポート番号を選択します。
☐ Use TLS/SSL	TLS/SSL を設定する場合、チェックボックスをオンにします。
☐ Use eMail Server Authentication	メールサーバ認証を使用する場合、ユーザー名とパスワードを入力します。
Email Group	現在、ご利用いただけません。
Performance Counter Alerts	
☐ Low Available License count bellow [x] %	使用可能なライセンス数を x %未満で指定します。
☐ Total Created Devices Exceeding	作成されたデバイスの合計が超過した場合
☐ Total Created Users Exceeding	作成されたユーザーの合計総数が超過した場合
☐ Database Connection Down	SQL に作成した SES データベースに接続できない場合
☐ Faild PBConnex Login Alert	プリブートネットワーク認証で、ログイン失敗した場合
☐ Application Event Log Full	アプリケーションイベントログが一杯にばった場合
☐ Device Added to Quarantine	デバイスが検疫に追加された場合
☐ Active Sessions Reaching Max	アクティブなセッションが最大値に達した場合
Email To:	メールの送信先アドレスを入力します。
Email From:	メールの送信元アドレスを入力します。
Email Subject:	メールの件名を入力します。
Send test	クリックするとメールの送信テストをおこなえます。
Encryption Status Alerts	
☐ Device entered Encrypting State	デバイスが暗号化状態になった
☐ Device entered Encrypted Reboot Required State	デバイスが暗号化されたリブート要求状態になった。
☐ Device entered Encrypted/Partially Encrypted State	デバイスが暗号化/部分暗号化状態になった。
☐ Device entered Decrypting State	デバイスが暗号化解除の状態になった。
☐ Device entered Decrypted/Plain Text State	デバイスが暗号化解除/プレーンテキスト状態に移行した。
Email To:	メールの送信先アドレスを入力します。

項　目	説　明
Email From:	メールの送信元アドレスを入力します。
Email Subject:	メールの件名を入力します。
Send test	クリックするとメールの送信テストをおこなえます。
Non-Communication Alerts	
☐ Enable Non-Communication Alerts	非通信アラートを有効にする場合、オンにします。
Email To:	メールの送信先アドレスを入力します。
Email From:	メールの送信元アドレスを入力します。
Email Subject:	メールの件名を入力します。
Send test	クリックするとメールの送信テストをおこなえます。

注　Non-Communication Alerts　を使用する場合、SES で下記の設定が必要です。

[SES] -> [Tools] -> [Options] -> [Other] -> Alert system

SCIM Sever

項　目	説　明
☐ Enable SCIM Server	クロスドメイン ID 管理システム（SCIM）仕様は、クラウドベースのアプリケーションおよびサービスにおけるユーザーID 管理を容易にするように設計されています。 SCIM サーバーを有効にします。 IdP が設定されている必要があります。 SCIM Client registration 登録パネルで<Add> ボタンをクリックして、追加します。
☐ Enable Detailed Trace	詳細なトレースログを有効にします。

17.3. ADSync 設定・機能一覧

General

項　目	説　明
Keyfile	
Keyfile path:	キーファイルを指定します。
Keyfile Password:	キーファイルのパスワードを入力します。
Database	
Server¥Instance:	SQL のインストールされているサーバー名とインスタンスを指定します。
Database:	接続するデータベース名を入力します。
◎ Windows Login	Windows 認証モードで、SQL に接続します。
○ SQL Server Login	SQL Server 認証モードで、SQL に接続します。
ADSync	
☐ Move deleted Users to Recycle Bin	削除したユーザーをごみ箱に移動します。
Logging	
☐ Log Events	イベントをログに記録します。
☐ Enable Detailed Trace to Folder	詳細ログを取得する場合、オンにします。 通常、オンにする必要はありません。サポートから詳細ログの要求があった場合に利用します。

ご注意